Basel Committee
on Banking Supervision

Consultative Document

Consolidated KYC Risk Management

Issued for comment by 30 October 2003

August 2003

BANK FOR INTERNATIONAL SETTLEMENTS

Table of Contents

Consolidated KYC Risk Management

Introduction

1. The adoption of effective know-your-customer (KYC) standards is an essential part of banks' risk management practices. As discussed in the *Customer due diligence for banks*[1] (CDD) paper, banks with inadequate KYC standards 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.

2. 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. To be truly effective, these elements should be adopted on a consolidated basis, encompassing the parent bank or head office[2] and all foreign branches and subsidiaries.

3. 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.

4. A global risk management programme for KYC should incorporate consistent identification and monitoring of customer accounts globally across business lines and geographical locations, as well as oversight at the parent level, in order to capture instances and patterns of unusual[3] transactions that might otherwise go undetected. Such comprehensive treatment of customer information can significantly contribute to a bank's overall reputational, concentration, operational and legal risk management through the detection of potentially harmful activities.

5. This paper describes the critical elements for effective consolidated KYC risk management.

Global process for managing KYC risks

6. The four essential elements of a sound KYC programme should be fully 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 its customer acceptance policy, procedures for customer identification, process for monitoring higher risk accounts and risk management framework on a global basis to all of its branches and subsidiaries around the world. The bank should clearly communicate those policies and procedures and ensure that they are fully adhered to. Where the minimum

---

1 Basel Committee on Banking Supervision, October 2001.

2 The term "head office" is used subsequently in this document to refer also to the parent bank.

3 The term "unusual" is used in this paper to refer also to "suspicious".

KYC standards of the home and host countries differ, offices in host jurisdictions should apply the higher standard of the two (CDD paragraph 66).

Customer acceptance policy

7. Banks 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. These policies and procedures for customer acceptance should be implemented consistently throughout the organisation.

Customer identification

8. A bank should establish a systematic procedure for identifying 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.

9. A bank should obtain appropriate identification information and maintain such information in a readily retrievable format so as to adequately identify its customers[4], 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.

10. Each office of the banking group should be in a position to comply with minimum identification and accessibility standards applied by the head office. However, some differences in information collection and retention may be necessary across jurisdictions to conform to local requirements or relative risk factors.

Monitoring of accounts and transactions

11. An essential element for addressing higher risks is the monitoring of customer account activity on a worldwide 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). Two of the approaches by which such monitoring may be accomplished are (1) the use of a centralised database; and (2) decentralised databases with robust information sharing between the head office and its branches and subsidiaries.

12. Under the first approach, accounts are monitored through the use of centralised databases of account balances, account activity and payments. This approach offers the advantage of permitting local and centralised monitoring across accounts in each office of the bank and facilitates monitoring of inter-office activity of customers with accounts in more than one office. However, because many foreign jurisdictions do not permit the routine transmission of customer data outside of their jurisdiction this approach may have limited applicability. An example of this practice can be seen in banks' monitoring of global payment activity, which has been facilitated by the establishment of centralised processing sites, i.e. payment "hubs".

---

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

13. Under the second approach, each office maintains and monitors information on its accounts and transactions. In this decentralised approach, 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. Information should flow both ways. Whilst the head office should inform the foreign branch or subsidiary of higher risk customers, the foreign branch or subsidiary should likewise be able to inform proactively the head office of higher risk relationships and other events that are relevant to the global management of reputational, legal, concentration and operational risk.

14. Regardless of the approach taken, banks should have policies and procedures for monitoring account activity for unusual transactions that are applied on a global basis. The procedures should be risk-based and emphasise the need to monitor both intra- and inter-country account activities.

Consolidated risk management and information sharing

15. 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, at a minimum, in accordance with the bank's global standards for customer identification, ongoing monitoring of accounts and transactions and the sharing of information.

16. Banks should ensure that their subsidiary and branch networks proactively provide information concerning higher risk customers and activities relevant to the global management of reputational, legal, concentration and operational risks, and respond to head office requests for account information in a timely manner. The bank's policies and procedures should describe the process to be followed for investigating and reporting unusual activity.

17. For information that is reported to the head office by a branch or subsidiary, head office should assess its world-wide exposure to the customer, and 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 unusual, detailing escalation procedures and guidance on restricting activities, including the closing of accounts as appropriate.

18. In addition to the proactive consolidated risk management processes, 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.

19. Banks' compliance and internal audit staffs, or external auditors, should evaluate adherence to all aspects of the global standards for KYC, including the requirements for sharing information with head office and responding to queries from head office related to higher risk and unusual account activities. The banking group's internal audit and compliance functions are the principal mechanism for monitoring the application of the bank's global KYC policies and procedures, including the effectiveness of the procedures for sharing information within the group

20. Where overseas offices are faced with host country laws that prevent compliance with the KYC standards of the home country, those offices should ensure that the head office and its home country supervisor are fully informed of the nature of the difference. Regarding such jurisdictions, banks should be aware of the higher reputational risk of conducting business in them, and should have a procedure for reviewing the vulnerability of the individual operating units, and implement additional safeguards where appropriate, including the possibility of closing down the operation (CDD paragraph 69).

Mixed financial groups

21. 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 reputation risk of the whole group.

22. 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.

The role of the supervisor

23. 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 some accounts (CDD paragraph 61).

24. In a cross-border context, home country supervisors or auditors should face no impediments in verifying the unit's compliance with KYC policies and procedures during on-site inspections. This will require a review of customer files and some random 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, while the home country supervisor is responsible for consolidated supervision of compliance with global KYC policies and procedures, the host country supervisor retains responsibility for the supervision of compliance with local KYC regulations.

25. The role of internal audit is particularly important in the evaluation of adherence to KYC standards on a consolidated basis and home country supervisors should ensure that they have effective access to any relevant reports carried out by internal audit.

26. Safeguards are needed to ensure that information regarding individual accounts is used exclusively for lawful supervisory purposes, and can be protected by the recipient in a satisfactory manner. A statement of mutual cooperation to facilitate information sharing between the two supervisors would be helpful in this regard (CDD paragraph 68).