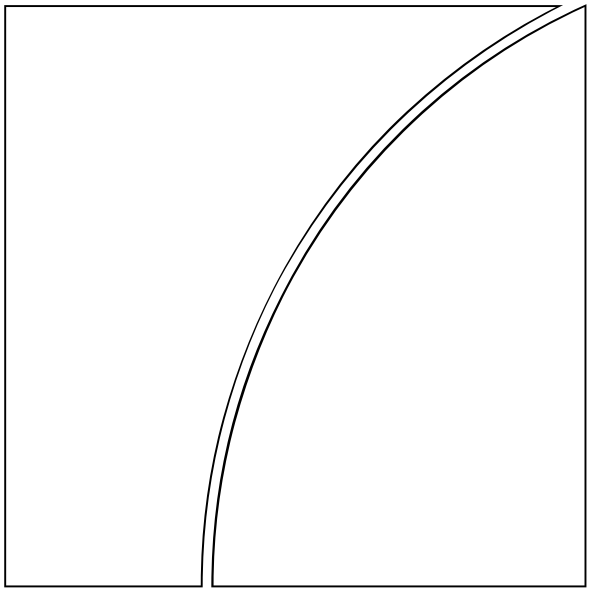
Basel Committee
on Banking Supervision



Consultative Document

Customer due diligence for banks

Issued for comment by 31 March 2001

January 2001

BANK FOR INTERNATIONAL SETTLEMENTS

Working Group on Cross-border Banking

Co-Chairs:

Mr Charles Freeland, Deputy Secretary General, Basel Committee on Banking Supervision

Mr Colin Powell, Chairman, Offshore Group of Banking Supervisors

Bermuda Monetary Authority	Mr D Munro Sutherland
Cayman Islands Monetary Authority	Mr John Bourbon Mrs Anna McLean
Commission Bancaire, France	Mr Laurent Ettori
Federal Banking Supervisory Office of Germany	Mr Jochen Sanio
Guernsey Financial Services Commission	Mr Peter G Crook
Banca d'Italia	Mr Giuseppe Godano
Financial Services Agency, Japan	Mr Kiyotaka Sasaki
Commission de Surveillance du Secteur Financier, Luxembourg	Mr Arthur Philippe
Monetary Authority of Singapore	Mrs Foo-Yap Siew Hong
Swiss Federal Banking Commission	Mr Daniel Zuberbühler Ms Dina Balleyguier
Financial Services Authority, United Kingdom	Mr Richard Chalmers
Board of Governors of the Federal Reserve System	Mr William Ryback
Federal Reserve Bank of New York	Ms Nancy Bercovici
Office of the Comptroller of the Currency	Mr Jose Tuya Ms Tanya Smith
Secretariat	Mr Luo Ping

Table of Contents

Customer due diligence for banks

Executive Summary

1. Supervisors around the world are increasingly recognising the importance of ensuring that their banks' have adequate controls and procedures in place so that they are not used for criminal or fraudulent purposes. Adequate due diligence on new and existing customers is a key part of these controls. Without this due diligence, banks can become subject to reputational, operational, legal and concentration risks which can result in significant financial cost to banks.

2. However, as a 1999 survey revealed, many supervisors around the world have not developed basic supervisory practices and are looking to the Basel Committee on Banking Supervision for insight on the appropriate steps to take. Accordingly, the Committee has developed a series of recommendations that provide a basic framework for supervisors and banks. Supervisors should work with their supervised institutions to ensure that these guidelines are considered in the development of know-your-customer (KYC) practices.

3. Anti-money laundering initiatives have traditionally been the province of the Financial Action Task Force (FATF) and it is not the Committee's intention to duplicate those efforts. Instead, the Committee's interest is from a wider prudential perspective. Sound KYC policies and procedures are critical in protecting the safety and soundness of banks and the integrity of banking systems.

4. The Basel Committee's previous guidance on customer due diligence and anti-money laundering efforts has been contained in three papers. *The Prevention of Criminal Use of the Banking System for the Purpose of Money-Laundering* was issued in 1988 and stipulates several basic principles, encouraging banks to identify customers, refuse suspicious transactions and cooperate with law enforcement agencies. The 1997 *Core Principles for Effective Banking Supervision* states that, as part of a sound internal control environment, banks should have adequate policies, practices and procedures in place that "promote high ethical and professional standards in the financial sector and prevent the bank from being used, intentionally or unintentionally, by criminal elements."[1] In addition, supervisors are encouraged to adopt the relevant recommendations of the FATF, relating to customer identification and record-keeping, reporting suspicious transactions, and measures to deal with countries with insufficient or no anti-money laundering measures. The 1999 *Core Principles Methodology* further elaborates the *Core Principles* by listing a number of essential and additional criteria.

5. Based on existing international KYC standards, national supervisors are expected to set out supervisory practice governing banks' KYC programmes. The essential elements as presented in this paper should provide clear guidance for supervisors to proceed with the work of designing or improving national supervisory practice:

(a) National supervisors are responsible for ensuring that banks have minimum standards and internal controls that allow them to adequately know their customers. Voluntary codes of conduct issued by industry organisations or associations are to

[1] Principle 15, *Core Principles for Effective Banking Supervision*

be encouraged but they are not in themselves sufficient to ensure market integrity or sound risk management. *(para 14)*

(b) A bank's KYC programme should include policies and procedures for customer acceptance, customer identification, on-going monitoring of high risk accounts and risk management. *(para 16)*

(c) Banks should develop clear customer acceptance policies and procedures, including a description of customers that should not be permitted to open accounts. Procedures should be in place for verifying the identity of new customers; banks should never enter into a business relationship until the identity is satisfactorily established. *(paras 17-19)*

(d) A bank should also undertake regular reviews of its customer base to ensure that it understands the nature of its accounts and the potential risks. *(para 20)*

(e) Banks offering private banking services are particularly vulnerable to reputational risk. The private banking operation should not function autonomously, or as a "bank within a bank", but should also be subject to KYC procedures. All new clients and new accounts should be approved by at least one person other than the private banker. If particular safeguards are in place internally to protect confidentiality of private banking customers and their business, banks must still ensure that these accounts are subject to appropriate scrutiny. *(para 21)*

(f) Banks should never open an account or conduct business with a customer who insists on anonymity or “bearer” status or who gives a fictitious name. In the case of confidential numbered accounts, the identities of the beneficiaries must be known to compliance staff, so that the due diligence process can be carried out satisfactorily. Banks also need to be vigilant in preventing corporate business entities from being used by natural persons as a method of operating anonymous accounts. *(paras 24-25)*

(g) Special issues related to the identification of the beneficial owner can arise in the case of trust, nominee, and fiduciary accounts. There are also issues with client accounts opened by professional intermediaries, and when banks use the services of introducers. The FATF is currently reviewing these issues, and the paper recognises the need to be consistent with the FATF. *(paras 27-32)*

(h) Business relationships with individuals holding important public positions and with persons or companies clearly related to them may expose a bank to significant reputational and/or legal risks when these persons are corrupt. Such persons, commonly referred to as “potentates”, include foreign heads of state, ministers, influential public officials, judges and military commanders. Decisions to enter into business relationships with potentates should be taken at senior management level, and banks should be particularly vigilant with respect to monitoring such accounts. It is incompatible with the fit and proper conduct of banking operations to accept or maintain a relationship if the bank knows or must assume that the funds derive from corruption or misuse of public assets. *(paras 17, 33 and 34)*

(i) Non-face-to-face account openings have increased significantly with the advent of postal, telephone and electronic banking. Banks are required to apply equally effective customer identification procedures and on-going monitoring standards for non-face-to-face customers as for those who are able to present themselves for interview. *(para 35)*

(j) The on-going monitoring of high risk accounts and transactions is an essential element of KYC. Banks should obtain and keep up-to-date customer identification papers, and retain them for at least five years after an account is closed. They should retain all financial transaction records for at least five years after the transaction has taken place. Banks should also have adequate information systems capable of monitoring customer accounts and potential suspicious patterns of activity. *(para 37)*

(k) The board of directors of a bank should be fully committed to an effective KYC programme, embracing policies and procedures for proper management oversight, systems and controls, segregation of duties, training and other related policies, including procedures for reporting suspicious transactions. The banks' internal audit and compliance functions should monitor the bank's compliance with these policies and procedures. *(paras 38 and 40)*

(l) Supervisors should ensure that banks have appropriate internal controls, are in compliance with supervisory guidance on KYC and take action to correct any deficiencies identified. Supervisors also need to take appropriate actions against those whose practices are inadequate. *(para 44-45)*

(m) All supervisors should expect banking groups to apply an acceptable minimum standard of policies and procedures to both their local and overseas operations. Where there are legal impediments in a host country to the implementation of higher home country KYC standards, host country supervisors should use their best endeavours to have the laws and regulations changed. In the meantime, overseas branches and subsidiaries should make sure the head office or parent bank and its home country supervisor are fully apprised of the situation. Where the problem is deemed to be sufficiently severe, supervisors should consider placing additional controls on banks operating in those jurisdictions and ultimately perhaps encouraging their withdrawal. *(paras 46-50)*

6. This paper is being released for consultation. Comments are invited from national supervisors and banks before 31 March 2001. These are to be sent to the Secretariat of the Basel Committee on Banking Supervision with copies to the national supervisory authorities, as appropriate.

I. Introduction

1. In reviewing the findings of an internal survey of cross-border banking in 1999, the Basel Committee identified deficiencies in a large number of countries' know-your-customer (KYC) policies for banks. Judged from a supervisory perspective, KYC policies in some countries have significant gaps and in others they are non-existent. Even among countries with well-developed financial markets, the extent of KYC robustness varies. Consequently, the Basel Committee asked the Working Group on Cross-border Banking[2] to examine the KYC procedures currently in place and to draw up recommended standards applicable to banks in all countries. This paper represents the findings and conclusions of the Working Group. The Basel Committee has endorsed the paper and is now distributing it worldwide in the expectation that the KYC framework presented here will become the benchmark for supervisors to establish national practices and for banks to design their own programmes.

2. KYC is most closely associated with the fight against money-laundering, which is essentially the province of the Financial Action Task Force (FATF).[3] While the Basel Committee continues to strongly support the adoption and implementation of the FATF recommendations, particularly those relating to banks, it also maintains that sound KYC procedures must be seen as a critical element in the effective management of banking risks. KYC safeguards go beyond simple account opening and record-keeping and require banks to formulate a customer acceptance policy and a tiered customer identification programme that involves more extensive due diligence for higher risk accounts, and includes proactive account monitoring for suspicious activities.

3. The Basel Committee's interest in sound KYC standards originates from its concerns for market integrity and has been heightened by the direct and indirect losses incurred by banks due to their lack of diligence in applying appropriate procedures. These losses could probably have been avoided and damage to the banks' reputation significantly diminished had the banks maintained effective KYC programmes.

4. This paper reinforces the principles established in earlier Committee papers by providing more precise guidance on the essential elements of KYC standards and their implementation. In developing this guidance, the Working Group has drawn on practices in member countries and taken into account evolving supervisory developments. The essential elements presented in this paper are guidance for worldwide implementation. In many cases, these standards may need to be supplemented and/or strengthened by further measures tailored to particular conditions and risks in the banking system of individual countries.

II. Importance of KYC standards for supervisors and banks

5. The FATF and other international groupings have worked intensively on KYC issues, and the FATF's Forty Recommendations on combating money-laundering[4] have

---

[2] This is a joint group consisting of members of the Basel Committee and the Offshore Group of Banking Supervisors.

[3] The FATF is an inter-governmental body which develops and promotes policies, both nationally and internationally, to combat money laundering. It has 29 member countries and two regional organisations. It works in close cooperation with other international bodies involved in this area such as the United Nations Office for Drug Control and Crime Prevention, the Council of Europe, the Asia-Pacific Group on Money Laundering and the Caribbean Financial Action Task Force.

[4] See FATF recommendations 10 to 19 which are reproduced in Annex 3.

international recognition and application. It is not the intention of this paper to duplicate that work.

6. At the same time, sound KYC procedures have particular relevance to the safety and soundness of banks, in that:

- they help to protect banks' reputation and the integrity of banking systems by reducing the likelihood of banks becoming a vehicle for or a victim of financial crime and suffering consequential reputational damage;

- they constitute an essential part of sound risk management (e.g. by providing the basis for identifying, limiting and controlling risk exposures in assets and liabilities, including assets under management).

7. The inadequacy or absence of KYC standards can subject banks to serious customer and counterparty risks, especially ***reputational, operational, legal and concentration risks***. It is worth noting that all these risks are interrelated. However, any one of them can result in a significant financial cost to banks (e.g. through the withdrawal of funds by depositors, the termination of inter-bank facilities, claims against the bank, investigation costs, asset seizures and freezes, and loan losses).

8. ***Reputational risk*** poses a major threat to banks, since the nature of their business requires maintaining the confidence of depositors, creditors and the general marketplace. Reputational risk is defined as the potential that adverse publicity regarding a bank's business practices, whether accurate or not, will cause a loss of confidence in the integrity of the institution. Banks are especially vulnerable to reputational risk because they can so easily become a vehicle for or a victim of illegal activities perpetrated by their customers. They need to protect themselves by means of continuous vigilance through an effective KYC programme.

9. ***Operational risk*** can be defined as the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events. Most operational risk in the KYC context relates to weaknesses in the implementation of banks' programmes, ineffective control procedures and failure to practise due diligence. A public perception that a bank is not able to manage its operational risk effectively can disrupt or adversely affect the business of the bank.

10. ***Legal risk*** is the possibility that lawsuits, adverse judgements or contracts that turn out to be unenforceable can disrupt or adversely affect the operations or condition of a bank. Banks may become subject to lawsuits resulting from the failure to observe mandatory KYC standards or from the failure to practise due diligence. Consequently, banks can, for example, suffer fines, criminal liabilities and special penalties imposed by supervisors. Indeed, a court case involving a bank may have far greater cost implications for its business than just the legal costs. Banks will be unable to protect themselves effectively from such legal risks if they do not engage in due diligence in identifying their customers and understanding their business.

11. Supervisory concern about ***concentration risk*** mostly applies on the assets side of the balance sheet. As a common practice, supervisors not only require banks to have information systems to identify credit concentrations but most also set prudential limits to restrict banks' exposures to single borrowers or groups of related borrowers. Without knowing precisely who the customers are, and their relationship with other customers, it will not be possible for a bank to measure its concentration risk. This is particularly relevant in the context of related counterparties and connected lending.

12. On the liabilities side, concentration risk is closely associated with funding risk, particularly the risk of early and sudden withdrawal of funds by large depositors, with potentially damaging consequences for the bank's liquidity. Concentration risk is more likely to be higher in the case of small banks and those that are less active in the wholesale markets than large banks. Analysing deposit concentrations naturally requires a bank to understand the characteristics of their depositors, including not only their identities but also the extent to which their actions may be linked with those of other depositors. It is essential that liabilities managers in small banks not only know but maintain a close relationship with large depositors, or they will run the risk of losing their funds particularly during emergencies.

13. It is also important to monitor concentration risk in assets under management. High net worth customers frequently have multiple accounts with the same bank, but in offices located in different countries. To effectively manage the reputational, compliance and legal risk arising from such accounts, banks should be able to aggregate and monitor balances and activity in these accounts on a global consolidated basis.

14. Both the Basel Committee and the Offshore Group of Banking Supervisors are fully convinced that effective KYC practices should be part of the risk management and internal control systems in all banks worldwide. National supervisors are responsible for ensuring that banks have minimum standards and internal controls that allow them to adequately know their customers. Voluntary codes of conduct[5] issued by industry organisations or associations are to be encouraged but they are not in themselves sufficient to ensure market integrity or sound risk management.

III. Essential elements of KYC standards

15. The Basel Committee's guidance on KYC has been contained in the following three papers and they reflect the evolution of the supervisory thinking over time. *The Prevention of Criminal Use of the Banking System for the Purpose of Money-Laundering* issued in 1988 stipulates the basic ethical principles and encourages banks to put in place effective procedures to identify customers, refuse suspicious transactions and cooperate with law enforcement agencies. The 1997 *Core Principles for Effective Banking Supervision* (CP) states, in a broader discussion of internal controls, that banks should have adequate policies, practices and procedures in place, including strict "know-your-customer" rules; specifically, supervisors should encourage the adoption of the relevant recommendations of the FATF. These relate to customer identification and record-keeping, increased diligence by financial institutions in detecting and reporting suspicious transactions, and measures to deal with countries with inadequate anti-money laundering measures. The 1999 *Core Principles Methodology* (CPM) further elaborates the Core Principles by listing a number of essential and additional criteria. (Annex 2 sets out the relevant extracts from the Core Principles and the Methodology.)

16. All banks should be required to "have in place adequate policies, practices and procedures that promote high ethical and professional standards and prevent the bank from being used, intentionally or unintentionally, by criminal elements".[6] Certain key elements should be included by banks in the design of KYC programmes that best suit their

---

[5] An example of an industry code is the "Global anti-money-laundering guidelines for Private Banking" (also called the Wolfsberg Principles) that was recently drawn up by twelve major banks with significant involvement in private banking.

[6] *Core Principles Methodology*, Essential Criterion 1.

circumstances. Such essential elements should start from the banks' risk management and control procedures and should include (1) customer acceptance policy, (2) customer identification, (3) on-going monitoring of high risk accounts and (4) risk management. Banks should not only establish the identity of their customers, but should also monitor account activity to determine those transactions that do not conform with the normal or expected transactions for that customer or type of account. KYC should be a core feature of banks' risk management and control procedures, and be complemented by regular compliance reviews and internal audit. Nonetheless, it is important that the requirements do not become so restrictive that they deny access to banking services, especially for people who are financially or socially disadvantaged. [7]

1. Customer acceptance policy

17. Banks should develop clear customer acceptance policies and procedures, including a description of the types of customer that are unacceptable to bank management. In preparing such policies, factors such as customers' background, country of origin, public or high profile position, business activities or other risk indicators should be considered. Banks should develop graduated customer acceptance policies and procedures that require more extensive due diligence for high risk customers. For example, the policies may require the most basic account-opening requirements for a working individual with a small account balance, whereas quite extensive due diligence may be deemed essential for an individual with a high net worth whose source of funds is unclear. Decisions to enter into business relationships with high risk customers, such as potentates (see below), should be taken exclusively at senior management level.

2. Customer identification

18. Customer identification is an essential element of KYC standards. A customer is defined as any person or entity that keeps an account with a bank and any person or entity on whose behalf an account is maintained, as well as the beneficiaries of transactions conducted by professional financial intermediaries. Specifically, a customer should include an account-holder and the beneficial owner of an account. A customer should also include the beneficiary of a trust, an investment fund, a pension fund or a company whose assets are managed by an asset manager, or the grantor of a trust.

19. Banks should establish a systematic procedure for verifying the identity of new customers and should never enter a business relationship until the identity of a new customer is satisfactorily established. Banks should "document and enforce policies for identification of customers and those acting on their behalf".[8] The best documents for verifying the identity of customers are those most difficult to obtain illicitly and to counterfeit. Special attention should be exercised in the case of non-resident customers and in no case should a bank short-circuit identity procedures just because the new customer is unable to present himself for interview. The bank should always ask itself why the customer has chosen to open an account in a foreign jurisdiction.

20. The customer identification process applies naturally at the outset of the relationship, but there is also a need to apply KYC standards to existing customer accounts.

---

[7] For example, it could be difficult for minors, students, the elderly and disabled people to produce the preferred documents confirming their identity.

[8] *Core Principles Methodology*, Essential Criterion 2.

Where such standards have been introduced only recently and do not as yet apply fully to existing customers, a risk assessment exercise can be undertaken and priority given to obtaining necessary information, where it is deficient, in respect of the higher risk cases. An appropriate time to review the information available on existing customers is when a transaction of significance takes place, or when there is a material change in the way that the account is operated. However, if a bank is aware that it lacks sufficient information about an existing high-risk customer, it should take steps to ensure that all relevant information is obtained as quickly as possible. In addition, the supervisor needs to set an appropriate target date for completion of a KYC review and regularisation of all existing accounts. In any event, a bank should undertake regular reviews of its customer base to establish that it has up-to-date information and a proper understanding of its account holders' identity and of their business.

21. Banks that offer private banking services are particularly exposed to reputational risk. Private banking by nature involves a large measure of confidentiality. Private banking accounts can be opened in the name of an individual, a commercial business, a trust, an intermediary or a personalised investment company. In each case reputational risk may arise if the bank does not diligently follow established KYC procedures. In no circumstances should private banking operations function autonomously, or as a "bank within a bank"[9], and no part of the bank should ever escape the required procedures. This means that all new clients and new accounts should be approved by at least one person other than the private banking relationship manager. If particular safeguards are put in place internally to protect confidentiality of private banking customers and their business, banks must still ensure that at least equivalent scrutiny and monitoring of these customers and their business can be conducted, e.g. they must be open to review by compliance officers and auditors.

2.1 General identification requirements

22. Banks need to obtain all information necessary to establish to their full satisfaction the identity of each new customer and the purpose and intended nature of the business relationship. The extent and nature of the information depends on the type of applicant (personal, corporate etc) and the expected size of the account. National supervisors are encouraged to provide guidance to assist banks in their designing their own identification procedures. Examples of the type of information that would be appropriate are set out in Annex 1.

23. Banks should apply their full KYC procedures to applicants that plan to transfer an opening balance from another financial institution, bearing in mind that the previous account manager may have asked for the account to be removed because of a concern about dubious activities.

24. Banks should never agree to open an account or conduct ongoing business with a customer who insists on anonymity or "bearer" status or who gives a fictitious name. Nor should confidential numbered[10] accounts function as anonymous accounts but they should be subject to exactly the same KYC procedures as all other customer accounts, even if the test is carried out by selected staff. Whereas a numbered account can offer additional protection for the identity of the account-holder, the identity must be known to a sufficient

---

[9] Some banks insulate their private banking functions or create Chinese walls as a means of providing additional protection for customer confidentiality.

[10] In a numbered account, the name of the beneficial owner is known to the bank but is substituted by an account number or code name in subsequent documentation.

number of staff to operate proper due diligence. Such accounts should in no circumstances be used to hide the customer identity from a bank's compliance function or from the supervisors.

25. Banks need to be vigilant in preventing corporate business entities from being used by natural persons as a method of operating anonymous accounts. Personal asset holding vehicles, such as international business companies (IBCs), may make proper identification of customers or beneficial owners difficult. A bank should take all steps necessary to satisfy itself that it knows the true identity of the ultimate owner of all such entities.

2.2 Specific identification issues

26. There are a number of more detailed issues relating to customer identification which need to be addressed. Particular comments are invited on the issues mentioned in this section. Several of these are currently under consideration by the FATF as part of a general review of its forty recommendations, and the Working Group recognises the need to be consistent with the FATF.

2.2.1 Trust, nominee and fiduciary accounts or client accounts opened by professional intermediaries

27. Trust, nominee and fiduciary accounts can be used to avoid customer identification procedures. While it may be legitimate under certain circumstances to provide an extra layer of security to protect the confidentiality of legitimate private banking customers, it is essential that the true relationship is understood. Banks should establish whether the customer is acting on behalf of another person as trustee, nominee or professional intermediary (e.g. a lawyer or an accountant). If so, a necessary precondition is receipt of satisfactory evidence of the identity of any intermediaries and of the persons upon whose behalf they are acting, as well as details of the nature of the trust or other arrangements in place.

28. Banks may hold "pooled" accounts (e.g. client accounts managed by law firms) or accounts opened on behalf of pooled entities, such as mutual funds and money managers. In such cases, banks have to decide, given the circumstances, whether the customer is the intermediary, or whether it would be more appropriate to look through the intermediary to the ultimate beneficial owners. In each case, the identity of the customer that is subject to due diligence should be clearly established. The beneficial owners should be verified where possible. Where not, the banks should perform due diligence on the intermediary and establish to its complete satisfaction that the intermediary has a sound due diligence process for each of its clients.

29. Special care needs to be exercised in initiating business transactions with companies that have nominee shareholders or shares in bearer form. Satisfactory evidence of the identity of beneficial owners of all companies needs to be obtained.

30. The above procedures may prove difficult for banks in some countries to follow. In the case of professional intermediaries such as lawyers, there might exist professional codes of conduct preventing the dissemination of information concerning their clients. The FATF is currently engaged in a review of KYC procedures governing accounts opened by lawyers on behalf of clients. The Working Group has therefore not taken a definitive position on this issue.

2.2.2 Introduced business

31. The performance of identification procedures can be time consuming and there is a natural desire to limit any inconvenience for new customers. In some countries, it has

therefore become customary for banks to rely on the procedures undertaken by other banks or introducers when business is being referred. In doing so, banks risk placing excessive reliance on the due diligence procedures that they expect the introducers to have performed. Relying on due diligence conducted by an introducer, however reputable, does not in any way remove the ultimate responsibility of the recipient bank to know its customers and their business. In particular, banks should not rely on introducers that are subject to weaker standards than those governing the banks' own KYC procedures or that are unwilling to share copies of due diligence documentation.

32. The FATF is currently engaged in a review of the appropriateness of eligible introducers, i.e. whether they should be confined to reputable banks only or should extend to other regulated institutions, whether a bank should establish a contractual relationship with its introducers and whether it is appropriate to rely on a third party introducer at all. The Working Group is still developing its thinking on this topic.

2.2.3 Potentate risk

33. Business relationships with individuals holding important public positions and with persons or companies clearly related to them may expose a bank to significant reputational and/or legal risks. Such persons, commonly referred to as "potentates", include foreign heads of state, ministers, influential public officials, judges and military commanders. There is always a possibility, especially in countries where corruption is widespread, that such persons abuse their public powers for their own illicit enrichment through the receipt of bribes, embezzlement, etc.

34. Accepting and managing funds from corrupt potentates will severely damage the bank's own reputation and can undermine public confidence in the ethical standards of an entire financial centre, since such cases usually receive extensive media attention and strong political reaction, even if the illegal origin of the assets is often difficult to prove. In addition, the bank may be subject to costly information requests and seizure orders from law enforcement or judicial authorities (including international mutual assistance procedures in criminal matters) and could be liable to actions for damages by the state concerned or the victims of a regime. Under certain circumstances, the bank and/or its officers and employees themselves can be exposed to charges of money laundering, if they know or should have known that the funds stemmed from corruption or other serious crimes. Indeed, some countries have recently amended or are in the process of amending their laws and regulations to criminalise active corruption of foreign civil servants and public officers in accordance with the relevant international convention.[11] In these jurisdictions foreign corruption becomes a predicate offence for money laundering and all the relevant anti-money laundering laws and regulations apply (e.g. reporting of suspicious transactions, prohibition on informing the customer, internal freeze of funds etc). But even in the absence of such an explicit legal basis in criminal law, it is clearly undesirable, unethical and incompatible with the fit and proper conduct of banking operations to accept or maintain a business relationship if the bank knows or must assume that the funds derive from corruption or misuse of public assets. There is a compelling need for banks considering a relationship with a potentate to identify that person as well as people and companies that are clearly related to the potentates.

[11] See OECD Convention on *Combating Bribery of Foreign Public Officials in International Business Transactions*, adopted by the Negotiating Conference on 21 November 1997.

2.2.4 Non-face-to-face customers

35. Banks are increasingly asked to open accounts on behalf of customers who do not present themselves for personal interview. This has always been a frequent event in the case of non-resident customers, but it has increased significantly with the recent advent of postal, telephone and electronic banking. Banks should apply equally effective customer identification procedures and on-going monitoring standards for non-face-to-face customers as for those available for interview. One issue that has arisen in this connection is the possibility of independent verification by a reputable third party. This whole subject of non-face-to-face customers is being discussed by the FATF, and is also the subject of a draft EC Directive, and the topic therefore remains subject to review by the Working Group.

36. A typical example of a non-face-to-face customer is one who wishes to conduct electronic banking via the Internet or similar technology. Electronic banking currently incorporates a wide array of products and services delivered over telecommunications networks. The anonymous and borderless nature of electronic banking combined with the speed of the transaction inevitably creates difficulty in customer identification and verification. As a basic policy, supervisors expect that banks should proactively assess various risks posed by emerging technologies and design customer identification procedures with due regard to such risks.[12]

3. On-going monitoring of high risk accounts

37. On-going monitoring of accounts and transactions is an essential aspect of effective KYC procedures. Banks can only effectively control and reduce their risk if they have an understanding of normal and reasonable account activity of their customers. Without such knowledge, they are likely to fail in their duty to report suspicious transactions to the appropriate authorities in cases where they are required to do so. The on-going monitoring process includes the following:

- Banks should develop “clear standards on what records must be kept on customer identification and individual transactions and the retention period”.[13] As the starting point and natural follow-up of the identification process, banks should obtain and keep up to date customer identification papers and retain them for at least five years after an account is closed. They should also retain all financial transaction records for at least five years after the transaction has taken place.

- Banks should ensure that they have adequate management information systems to provide managers and compliance officers with timely information needed to identify, analyse and effectively monitor higher risk customer accounts. The types of reports that may be needed include reports of missing account opening documentation, transactions made through a customer account that are unusual, and aggregations of a customer’s total relationship with the bank.

- Senior management of a bank in charge of private banking business should know the personal circumstances of the bank’s large/important customers and be alert to

---

[12] The Electronic Banking Group of the Basel Committee is currently developing guiding principles for the prudent risk management of electronic banking activities and will specifically outline appropriate supervisory expectations regarding the approaches banks should take in identifying, assessing, managing and controlling the risks associated with electronic banking. These principles will also include guidance on how to authenticate and identify customers in an electronic banking context.

[13] Core Principles Methodology, Essential Criterion 2

sources of third party information. Every bank should draw its own distinction between large/important customers and others, and set threshold indicators for them accordingly, taking into account the country of origin and other risk factors. Significant transactions by high risk customers should be approved by a senior manager.

- Banks should have systems in place to detect unusual or suspicious patterns of activity. This can be done by establishing limits for a particular class or category of accounts. Particular attention should be paid to transactions that exceed these limits. Certain types of transactions should alert banks to the possibility that the customer is conducting undesirable activities. They may include transactions that do not make economic or commercial sense, or that involve large amounts of cash deposits that are not consistent with the normal and expected transactions of the customer. Very high account turnover, inconsistent with the size of the balance, may indicate that funds are being "washed" through the account. A list of suspicious activities drawn up by supervisors can be very helpful to banks.

- Banks should develop a clear policy and internal guidelines, procedures and controls and remain especially vigilant regarding business relationships with potentates and high profile individuals or with persons and companies that are clearly related to or associated with them.[14]

4. Risk management

38. Effective KYC procedures embrace routines for proper management oversight, systems and controls, segregation of duties, training and other related policies. The board of directors of the bank should be fully committed to an effective KYC programme by establishing appropriate procedures and ensuring their effectiveness. Banks should appoint a senior officer with explicit responsibility for ensuring that the bank's policies and procedures are, at a minimum, in accordance with local supervisory practice. Banks should have clear written procedures, communicated to all personnel, for staff to report suspicious transactions to a specified senior manager. That manager must then assess whether the bank's statutory obligations under recognised suspicious activity reporting regimes require the transaction to be reported to the appropriate law enforcement and supervisory authorities.

39. All banks must have an ongoing employee-training programme so that bank staff is adequately trained in KYC procedures. The timing and content of training for various sectors of staff will need to be adapted by the bank for its own needs. Training requirements should have a different focus for new staff, front-line staff, compliance staff or staff dealing with new customers. New staff should be educated in the importance of KYC policies and the basic requirements at the bank. Front-line staff members who deal directly with the public should be trained to verify the customer identity for new customers, to exercise due diligence in handling accounts of existing customers on an ongoing basis and to detect patterns of suspicious activity. Regular refresher training should be provided to ensure that staff is reminded of their responsibilities and is kept informed of new developments. It is crucial that all relevant staff fully understand the need for and implement KYC policies consistently. A

[14] It is unrealistic to expect the bank to know or investigate every distant family, political or business connection of a foreign customer. The need to pursue suspicions will depend on the size of the assets or turnover, pattern of transactions, economic background, reputation of the country, plausibility of the customer's explanations etc. It should however be noted that potentates (or rather their family members and friends) would not necessarily present themselves in that capacity, but rather as ordinary (albeit wealthy) business people, masking the fact they owe their high position in a legitimate business corporation only to their privileged relation with the holder of the public office.

culture within banks that promotes such understanding is the key to successful implementation.

40. Banks' internal audit and compliance functions have important responsibilities in evaluating and ensuring adherence to KYC policies and procedures. As a general rule, the compliance function provides an independent evaluation of the bank's own policies and procedures, including legal and regulatory requirements. Its responsibilities should include ongoing monitoring of staff performance through sample testing of compliance and review of exception reports to alert senior management or the Board of Directors if it believes management is failing to address KYC procedures in a responsible manner.

41. Internal audit plays an important role in independently evaluating the risk management and controls, discharging its responsibility to the Audit Committee of the Board of Directors or a similar oversight body through periodic evaluations of the effectiveness of compliance with KYC policies and procedures. Management should ensure that audit functions are staffed adequately with individuals who are well-versed in such policies and procedures. In addition, internal auditors should be proactive in following-up their findings and criticisms.

42. In many countries, external auditors also have an important role to play in monitoring banks' internal controls and procedures, and in confirming that they are in compliance with supervisory practice.

IV. The role of supervisors

43. Based on existing international KYC standards, national supervisors are expected to set out supervisory practice governing banks' KYC programmes. The essential elements as presented in this paper should provide clear guidance for supervisors to proceed with the work of designing or improving national supervisory practice.

44. In addition to setting out the basic elements for banks to follow, supervisors have a responsibility to monitor that banks are applying sound KYC procedures and are sustaining ethical and professional standards on a continuous basis. Supervisors should ensure that appropriate internal controls are in place and that banks are in compliance with supervisory 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. Supervisors should always have the right to access all documentation related to accounts maintained in that jurisdiction, including any analysis the bank has made to detect suspicious transactions.

45. Supervisors have a duty not only to ensure their banks maintain high KYC standards to protect their own safety and soundness but also to protect the integrity of their national banking system. Supervisors should make it clear that they will take appropriate action, which may be severe and public if the circumstances warrant, against banks and their officers who demonstrably fail to follow their own internal procedures. In addition, supervisors should ensure that banks are aware of and pay particular attention to transactions that involve jurisdictions where standards are considered inadequate. The FATF and some national authorities have listed a number of countries and jurisdictions that are considered to have legal and administrative arrangements that do not comply with international standards for combating money laundering. Such findings should be a component of a bank's KYC policies and procedures.

V. Implementation of KYC standards in a cross-border context

46. Supervisors around the world should seek, to the best of their efforts, to construct and implement their national KYC standards fully in line with international standards so as to avoid potential regulatory arbitrage and safeguard the integrity of domestic and international banking systems. The implementation and assessment of such standards put to the test the willingness of supervisors to cooperate with each other in a very practical way, as well as the ability of banks to control risks on a groupwide basis. This is a challenging task for banks and supervisors alike.

47. Supervisors expect banking groups to apply an accepted minimum standard of KYC policies and procedures to both their local and overseas operations. The supervision of international banking can only be effectively carried out on a consolidated basis, and reputational risk as well as other banking risks are not limited to national boundaries. Parent banks must communicate their policies and procedures to their overseas branches and subsidiaries, including non-banking entities such as private trust companies, and have a routine for testing compliance against both home and host country KYC standards in order for their programmes to operate effectively globally. Such compliance tests will also be tested by external auditors and supervisors. Therefore, it is important that KYC documentation is properly filed and available for their inspection. As far as compliance checks are concerned, supervisors and external auditors will in most cases wish to examine systems and controls and look at customer accounts and transactions monitoring as part of a sampling process.

48. However small an overseas establishment is, a senior officer should be designated to be directly responsible for ensuring that all relevant staff are trained in, and observe, KYC procedures that meet both home and host standards. While this officer will bear primary responsibility, he should be supported by internal auditors and compliance officers from both local and head offices as appropriate.

49. Where the minimum KYC standards of the home and host countries differ, branches and subsidiaries in the host jurisdictions should apply the higher standard of the two. In general, there should be no impediment to prevent a bank from adopting standards that are higher than the minima required locally. If, however, local laws and regulations (especially secrecy provisions) prohibit the implementation of home country KYC standards, where the latter are more stringent, host country supervisors should use their best endeavours to have the law and regulations changed. In the meantime, overseas branches and subsidiaries would have to comply with host country standards, but they should make sure the head office or parent bank and its home country supervisor are fully informed of the nature of the difference.

50. Criminal elements are likely to be drawn toward jurisdictions with such impediments. Hence, banks should be aware of the high reputational risk of conducting business in these jurisdictions. Parent banks should have a procedure for reviewing the vulnerability of the individual operating units and implement additional safeguards where appropriate. In extreme cases, supervisors should consider placing additional controls on banks operating in those jurisdictions and ultimately perhaps encouraging their withdrawal.

51. During on-site inspections, home country supervisors or auditors should face no impediments in verifying the unit's compliance with KYC policies and procedures. 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. Where the home country supervisor requires consolidated reporting of deposit or borrower concentrations or notification of funds under management, there should be no

impediments. In addition, with a view to monitoring deposit concentrations or the funding risk of the deposit being withdrawn, home supervisors may apply materiality tests and establish some thresholds so that if a customer's deposit exceeds a certain percentage of the balance sheet, banks should report it to the home supervisor. However, safeguards are needed to ensure that information on individual accounts is used for supervisory purposes only and not passed on to non-supervisory third parties.

52. In certain cases there may be a serious conflict between the KYC policies of a parent bank imposed by its home authority and what is permitted in a cross-border office. There may, for example, be local laws that prevent inspections by the parent banks' compliance officers, internal auditors or home country supervisors, or that enable bank customers to use fictitious names or to hide behind agents or intermediaries that are forbidden from revealing who their clients are. In such cases, the home supervisor is recommended to communicate with the host supervisor in order to confirm whether there are indeed genuine legal impediments and whether they apply extraterritorially. If they prove to be insurmountable, 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. In the final analysis, any arrangements underpinning such on-site examinations should provide a mechanism that permits an assessment that is satisfactory to the home supervisor. Statements of cooperation or memoranda of understanding setting out the mechanics of the arrangements may be helpful. Access to information by home country supervisors should be as unrestricted as possible, covering banks' general policies and procedures for customer due diligence and for dealing with suspicions.

VI. Consultation process

53. This paper is being released for consultation. Comments are invited from national supervisors, relevant international organisations and banks by 31 March 2001, after which the final document will be issued. Comments should be sent to the Secretariat of the Basel Committee on Banking Supervision (Address: The Basel Committee on Banking Supervision, Bank for International Settlements, CH-4002 Basel, Switzerland; Fax: 41 61 2809100) with copies to the national supervisory authorities, as appropriate.

Annex 1

General identification requirements

This annex presents a suggested list of identification requirements for personal customers and corporates. National supervisors are encouraged to provide guidance to assist banks in designing their own identification procedures.

Personal customers

For personal customers, banks need to obtain the following information:

- name and/or names used,
- permanent residential address,
- date and place of birth,
- name of employer or nature of self-employment/business
- specimen signature, and
- source of funds.

Additional information would relate to nationality or country of origin, public or high profile position, etc. Banks should verify the information against original documents of identity issued by an official authority (examples including identity cards and passports). Such documents should be those that are most difficult to obtain illicitly. In countries where new customers do not possess the prime identity documents, eg, identity cards, passports or driving licences, some flexibility may be required. However, particular care should be taken in accepting documents that are easily forged or which can be easily obtained in false identities. Where there is face to face contact, the appearance should be verified against an official document bearing a photograph. Any subsequent changes to the above information should also be recorded and verified.

Corporate and other business customers

For corporate and other business customers, banks should obtain evidence of their legal status, such as an incorporation document, partnership agreement, association documents or a business licence. For large corporate accounts, a financial statement of the business or a description of the customer's principal line of business should also be obtained. In addition, if significant changes to the company structure or ownership occur subsequently, further checks should be made. In all cases, banks need to verify that the corporation or business entity exists and engages in its stated business. The original documents or certified copies of certificates should be produced for verification.

Annex 2

Excerpts from *Core Principles Methodology*

Principle 15: Banking supervisors must determine that banks have adequate policies, practices and procedures in place, including strict "know-your-customer" rules, that promote high ethical and professional standards in the financial sector and prevent the bank being used, intentionally or unintentionally, by criminal elements.

Essential criteria

1. The supervisor determines that banks have in place adequate policies, practices and procedures that promote high ethical and professional standards and prevent the bank from being used, intentionally or unintentionally, by criminal elements. This includes the prevention and detection of criminal activity or fraud, and reporting of such suspected activities to the appropriate authorities.

2. The supervisor determines that banks have documented and enforced policies for identification of customers and those acting on their behalf as part of their anti-money-laundering program. There are clear rules on what records must be kept on customer identification and individual transactions and the retention period.

3. The supervisor determines that banks have formal procedures to recognise potentially suspicious transactions. These might include additional authorisation for large cash (or similar) deposits or withdrawals and special procedures for unusual transactions.

4. The supervisor determines that banks appoint a senior officer with explicit responsibility for ensuring that the bank's policies and procedures are, at a minimum, in accordance with local statutory and regulatory anti-money laundering requirements.

5. The supervisor determines that banks have clear procedures, communicated to all personnel, for staff to report suspicious transactions to the dedicated senior officer responsible for anti-money laundering compliance.

6. The supervisor determines that banks have established lines of communication both to management and to an internal security (guardian) function for reporting problems.

7. In addition to reporting to the appropriate criminal authorities, banks report to the supervisor suspicious activities and incidents of fraud material to the safety, soundness or reputation of the bank.

8. Laws, regulations and/or banks' policies ensure that a member of staff who reports suspicious transactions in good faith to the dedicated senior officer, internal security function, or directly to the relevant authority cannot be held liable.

9. The supervisor periodically checks that banks' money laundering controls and their systems for preventing, identifying and reporting fraud are sufficient. The supervisor has adequate enforcement powers (regulatory and/or criminal prosecution) to take

action against a bank that does not comply with its anti-money laundering obligations.

10. The supervisor is able, directly or indirectly, to share with domestic and foreign financial sector supervisory authorities information related to suspected or actual criminal activities.

11. The supervisor determines that banks have a policy statement on ethics and professional behaviour that is clearly communicated to all staff.

Additional criteria

1. The laws and/or regulations embody international sound practices, such as compliance with the relevant forty Financial Action Task Force Recommendations issued in 1990 (revised 1996).

2. The supervisor determines that bank staff is adequately trained on money laundering detection and prevention.

3. The supervisor has the legal obligation to inform the relevant criminal authorities of any suspicious transactions.

4. The supervisor is able, directly or indirectly, to share with relevant judicial authorities information related to suspected or actual criminal activities.

5. If not performed by another agency, the supervisor has in-house resources with specialist expertise on financial fraud and anti-money laundering obligations.

Annex 3

Excerpts from FATF recommendations

C. Role of the financial system in combating money laundering

Customer Identification and Record-keeping Rules

10. Financial institutions should not keep anonymous accounts or accounts in obviously fictitious names: they should be required (by law, by regulations, by agreements between supervisory authorities and financial institutions or by self-regulatory agreements among financial institutions) to identify, on the basis of an official or other reliable identifying document, and record the identity of their clients, either occasional or usual, when establishing business relations or conducting transactions (in particular opening of accounts or passbooks, entering into fiduciary transactions, renting of safe deposit boxes, performing large cash transactions).

    In order to fulfil identification requirements concerning legal entities, financial institutions should, when necessary, take measures:

    (i) to verify the legal existence and structure of the customer by obtaining either from a public register or from the customer or both, proof of incorporation, including information concerning the customer's name, legal form, address, directors and provisions regulating the power to bind the entity.

    (ii) to verify that any person purporting to act on behalf of the customer is so authorised and identify that person.

11. Financial institutions should take reasonable measures to obtain information about the true identity of the persons on whose behalf an account is opened or a transaction conducted if there are any doubts as to whether these clients or customers are acting on their own behalf, for example, in the case of domiciliary companies (i.e. institutions, corporations, foundations, trusts, etc. that do not conduct any commercial or manufacturing business or any other form of commercial operation in the country where their registered office is located).

12. Financial institutions should maintain, for at least five years, all necessary records on transactions, both domestic or international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of criminal behaviour.

    Financial institutions should keep records on customer identification (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence for at least five years after the account is closed.

    These documents should be available to domestic competent authorities in the context of relevant criminal prosecutions and investigations.

13. Countries should pay special attention to money laundering threats inherent in new or developing technologies that might favour anonymity, and take measures, if needed, to prevent their use in money laundering schemes.

Increased Diligence of Financial Institutions

14. Financial institutions should pay special attention to all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. The background and purpose of such transactions should, as far as possible, be examined, the findings established in writing, and be available to help supervisors, auditors and law enforcement agencies.

15. If financial institutions suspect that funds stem from a criminal activity, they should be required to report promptly their suspicions to the competent authorities.

16. Financial institutions, their directors, officers and employees should be protected by legal provisions from criminal or civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report their suspicions in good faith to the competent authorities, even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred.

17. Financial institutions, their directors, officers and employees, should not, or, where appropriate, should not be allowed to, warn their customers when information relating to them is being reported to the competent authorities.

18. Financial institutions reporting their suspicions should comply with instructions from the competent authorities.

19. Financial institutions should develop programs against money laundering. These programs should include, as a minimum:

    (i) the development of internal policies, procedures and controls, including the designation of compliance officers at management level, and adequate screening procedures to ensure high standards when hiring employees;

    (ii) an ongoing employee training programme;

    (iii) an audit function to test the system.