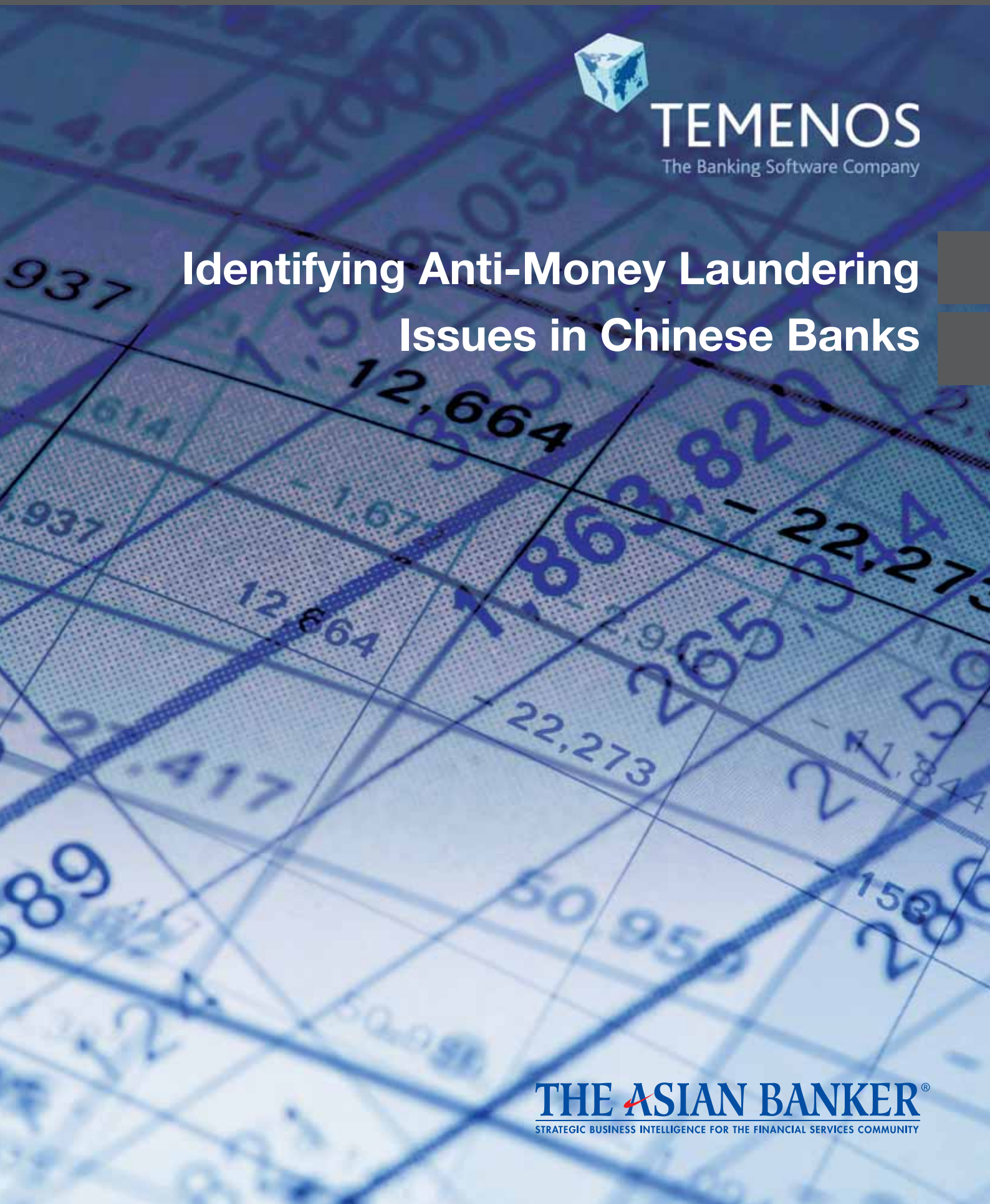
Asian Banker Research



TEMENOS
The Banking Software Company

Identifying Anti-Money Laundering Issues in Chinese Banks

THE ASIAN BANKER®
STRATEGIC BUSINESS INTELLIGENCE FOR THE FINANCIAL SERVICES COMMUNITY

Table of Contents

Introduction

Anti-Money Laundering (AML) has grown to significant importance for financial institutions around the globe. Non-compliance with government regulations can cause significant reputational damage and penalties. As large-volume transactions are common in the wealth management business, regulators keep a close eye on the premium banking segment of financial institutions. It is crucial for banks to develop solid AML and Counter Terrorist Financing (CTF) capabilities to manage these risks. The director of retail banking in a Chinese big four bank told us in an interview that international cooperation combined with the rendering of perfect internal guidelines, the installation of modern technologies and a strengthening of human resource training programmes will be the key for Chinese banks to counter international financial crime.

AML was introduced in China as a result of regulatory change, and Chinese banks were pressured into action. This resulted in hasty and ineffectual implementation of first generation IT, processes and training. So far, only few Chinese banks have moved beyond this point.

In particular, the reporting and analysis of suspicious transactions is still a largely ineffective process. Although the formal banking sector made progress in tracking financial transactions connected with money laundering or terrorist financing, the sheer size of the informal financial services industry and the large numbers of underground banks make effective AML/CTF a difficult endeavour in China.

Adequate internal control mechanisms and administrative rules, beyond regulatory requirements, have not been established in most Chinese commercial banks. Structural changes inside the banks, such as in company culture, comprehensive training and an understanding of the importance of AML practices remains largely absent in many banks and in peripheral branches.

Development of the AML regulatory regime in China

China has made considerable regulatory progress in developing its AML and CTF regime in the last five years. This includes legislative reform, the strengthening of enforcement mechanisms, and implementing international cooperation initiatives. These days, Chinese authorities keep a closer eye on corruption and bribery, which remain the majority of AML-related investigations.

Money laundering however continues to be a serious concern as it involves funds from narcotics trafficking, smuggling, trafficking of persons, counterfeiting of trade goods, fraud, tax evasion, corruption, and other financial crimes. Proceeds of tax evasion are recycled through offshore companies and return to China disguised as foreign investment and thus receive tax benefits. Particularly challenging for combating AML is the unenforceability of the unofficial banking system as well as the cash-based economy.

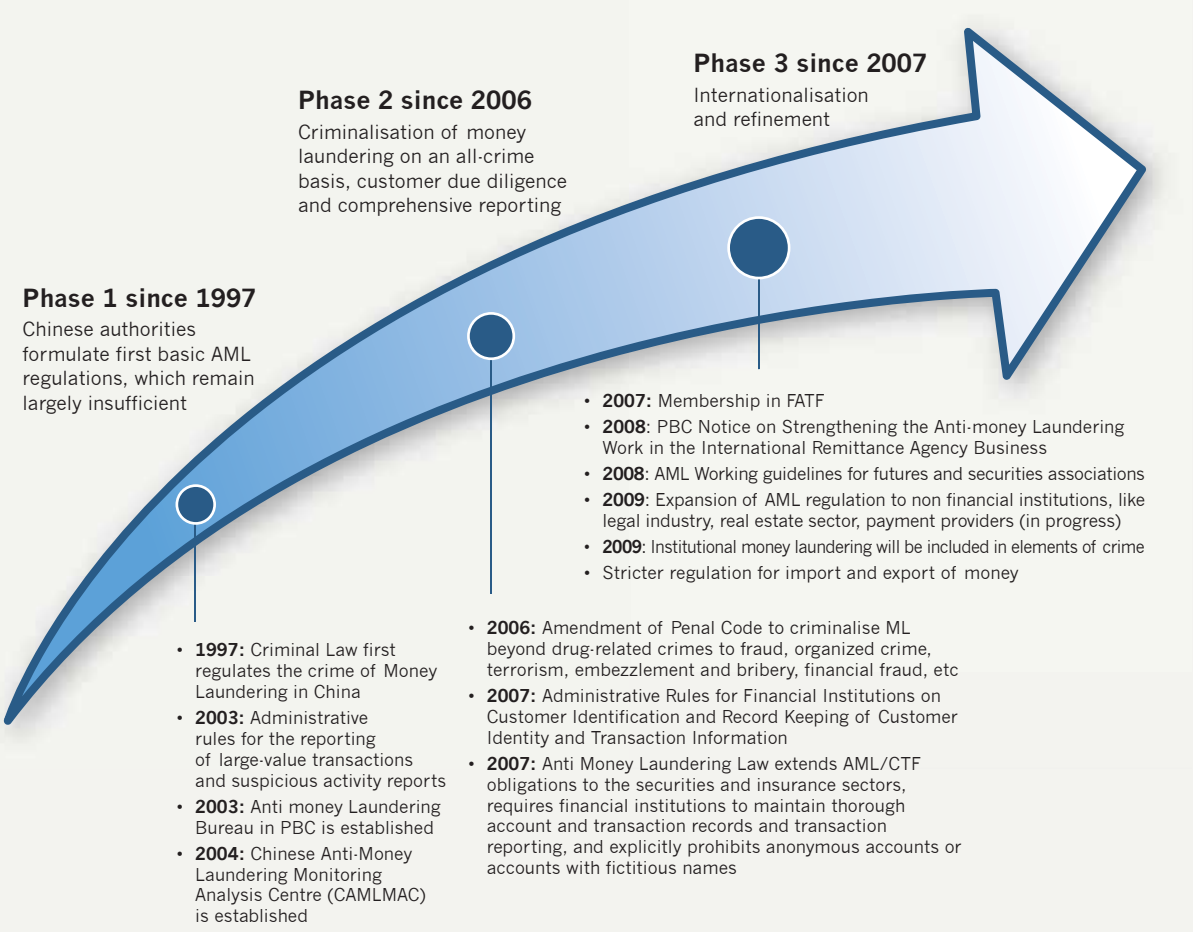
AML controls in China are fragmented and often overlapping, making effective combating difficult. The main controlling body against money laundering in China is the People's Bank of China (PBOC) and in particular, the Anti-Money Laundering Bureau, which is the field investigative body of the PBOC. It controls the AML mechanisms in banks, and conducts on-premise controls and various trainings for them. Secondly, the PBOC runs the Chinese Anti-Money Laundering Monitoring Analysis Centre (CAMLMAC), which is the financial information unit (FIU) in China. The CAMLMAC is responsible for collecting, analysing and reporting large-value and suspicious transactions.

The PBOC shares some responsibilities with other regulatory bodies such as the China Banking Regulatory Commission (CBRC), China Insurance Regulatory Commission (CIRC), and China Securities Regulatory Commission (CSRC). The Ministry of Public Security (MPS) has both an AML Division and an Anti-Terrorism Bureau, which lead AML and CTF-related law enforcement efforts.

The institutionalisation of the AML regime in 2007 marks a major milestone in China. The AML Law requires financial institutions to report large and suspicious transactions. It also includes hitherto-unregulated sectors like securities and insurances into the AML regime. In line with this, the People's Bank of China revised its AML/CFT regulatory framework by launching the Rules for AML by Financial Institutions and the

Figure 1.1

Development of AML regulatory regime in China



Source: Asian Banker Research

Administrative Rules for Reporting of Large-Value and Suspicious Transactions by Financial Institutions, which marks a milestone as these rules require financial institutions to file suspicious transactions reports related to terrorist financing.

In August 2007, China adopted the Administrative Rules for Financial Institutions on Customer Identification and Record Keeping of Customer Identity and Transaction Information, requiring all financial institutions to identify and verify their customers, including the beneficial owner. The new rules oblige banks to report any cash deposit or withdrawal of over RMB 200,000 ($27,000) or foreign-currency withdrawals of over $10,000 in one business day to the PBOC's financial intelligence unit (FIU), the CAMLMAC. Money transfers exceeding RMB 2 million ($274,000) between companies in one day or between an individual and a company greater than RMB 500,000 ($69,000) are also to be reported. The reports must be communicated to the FIU either electronically within five days or in writing within 10 days. Furthermore banks have to deliver monthly reports describing suspicious activities and retain transaction records for five years. Cash transactions however, such as cash transfers and cash exchanges are not included in the money laundering schemes and therefore also bear potential opportunities for money launderers.

The regulations of the PBOC identify 23 standards for suspicious activities that have to be reported both to the CAMLMAC and also to local law enforcement authorities.

There are several standards, which tend to launch a higher amount of alerts and thus are more difficult to deal with. These are transactions, which are just below the threshold levels, which do not match the customer profile or whose source is suspicious or not verifiable. Above that, renewed account activity of

a dormant account or early repayment of loans also triggers various alerts.

China also enhanced the criminalisation of money laundering in its penal code by including money from other offences such as narcotics trafficking, smuggling, organized crime, terrorism, embezzlement and bribery, financial fraud and disrupting the financial management order as part of the scope of what transacted funds are considered as money laundering. This criminalises money laundering on the basis of an all-crimes approach and complicity in concealing the proceeds of criminal activity.

However, there are several aspects where Chinese regulation does not meet international standards yet. China has increased its efforts to counter terrorists. The government now has the authority to identify, freeze, and seize terrorist financial assets. But the laws concerning terrorist financing are not yet consistent with international standards, according to a report by the Financial Action Task Force (FATF) in 2007/2008.

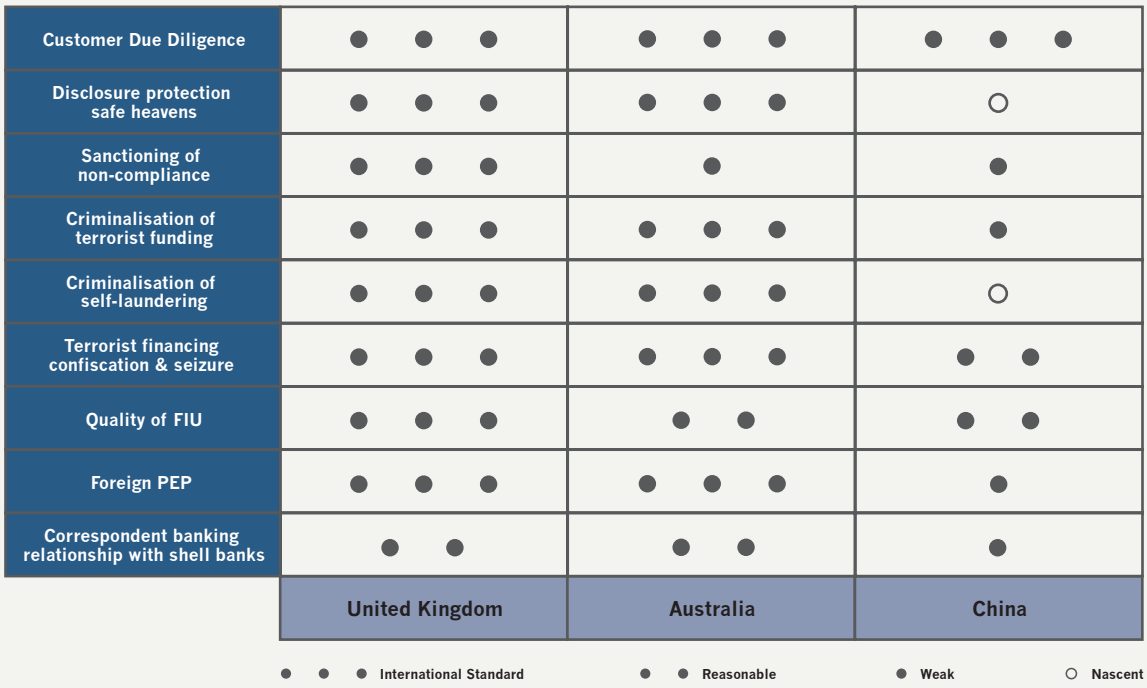
Hitherto, Chinese law has not criminalised the activity of collecting funds for terrorists or terrorist organizations for the purpose of committing a terrorist act or any other purpose. Another key weakness is China's terrorist financing confiscation and seizure regime, which lacks the full implementation of United Nations Security Council Resolution (UNSCR) 1267 and UNSCR 1373. China's last FATF evaluation states that China's seizure regime does not sufficiently and adequately respond to the freezing designations set out in the relevant United Nations resolutions. China has

"Most financial institutions have to focus on real-time detection, rather than post supervision, which results in the fact that detection is mostly limited to deposit and withdrawals over the counter"

AML Bureau in People's Bank of China

Figure 1.2

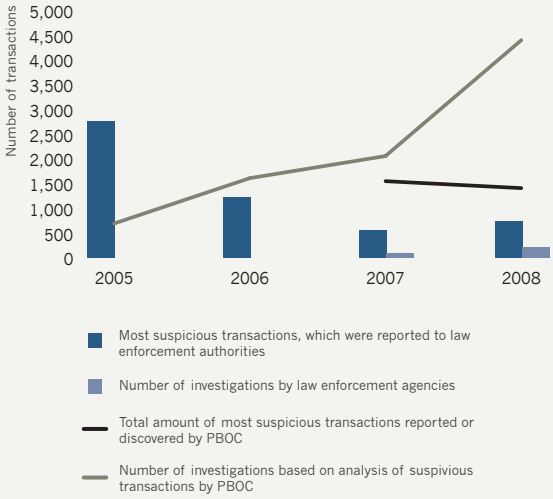
Assessment of China's regulatory AML regime



Source: Asian Banker Research

Figure 1.3

Increased investigative efforts by the PBOC, despite a falling number of suspicious transactions in general, also lead to higher activity by law enforcement agencies



Source: Asian Banker Research

"no clear determination of the scope of the freezing obligations in respect to what assets need to be targeted and their link with the terrorist individuals and entities", according to the FATF report.

Another issue which has not been properly addressed, as it has not yet been criminalised, is self laundering, where an offender simply acts to launder the proceeds of his own offending. China furthermore lacks explicit requirements in its AML law for financial institutions to have an adequate audit function to test compliance with internal AML/CFT controls. The AML Law does not require financial institutions to provide relevant employees with CFT training.

Public reporting and transparency are another major deficiency of the Chinese authorities. Publicly available information is mostly antiquated and not easy to retrieve. English versions of authorities' websites contain even more limited information compared to the already insufficient Chinese sites.

It would seem that China has a sufficiently comprehensive AML regulatory regime in place. So the problem is not the absence of regulation, but rather the enforcement of law. Chinese authorities and banks, like in many other countries in Asia, follow AML regulation rather by form and not by spirit. Non-compliance with customer due diligence (CDD) requirements is widespread.

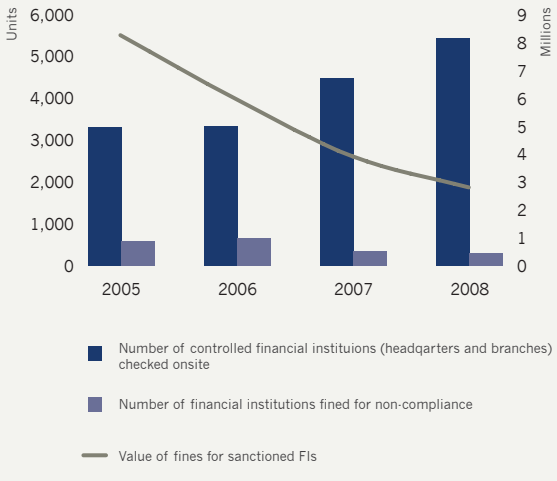
For an institution to be found non-compliant, it is not even necessary to be involved in money laundering. If the institution does not, in the regulators view, have effective systems and controls to provide reasonable assurance that the institutions can avoid aiding or abetting money launderers, the regulator can take action. It can impose fines between US$30,000 and US$ 70,000, on the institution for misconduct. Directors, senior managers and other persons directly responsible for the misconduct can also receive a fine between US$1500 and US$ 7300. If non-compliance leads to actual money laundering, the fines are about ten times higher.

In 2008 the PBOC checked 5,504 financial institutions (headquarters and branches) on-site, of which 304 were fined for non-compliance. The fines amounted to US$1.3 million, leaving banks with an average fine of about US$ 4,000. This indicates the PBOC's light handed stance on the enforcement of AML violations. Additionally, 60 managerial individuals were held directly accountable for misconducts and were fined.

However in order to create a genuine incentive for banks to reduce money laundering, the regulator must be willing to legislate and execute serious punishment to improve credibility. Otherwise banks will not make the effort to sustainably reduce money laundering.

Figure 1.4

Despite more stringent regulatory controls, Chinese banks incurred lesser convictions and fines



Source: Asian Banker Research

Development of AML capabilities in Chinese banks

With the new regulations, banks sought rapid compliance which did not necessarily result in efficient capabilities to fight money laundering. The regulator's push for AML was the main driver for the implementation of AML operations, but a deeper understanding for the necessity of AML and CTF could neither be conveyed to the financial institutions in China nor to their employees.

Almost all Chinese banks have more or less successfully implemented Phase 1, but achieving Phase 2 is challenging and often not a major priority. For this reason only a few more sophisticated banks made it to Phase 2 so far. Several foreign banks can be placed in Phase 3, as they utilise the IT and processes of their international groups, whereas a few best practice banks, such as DBS, entered Phase 4 on a global level.

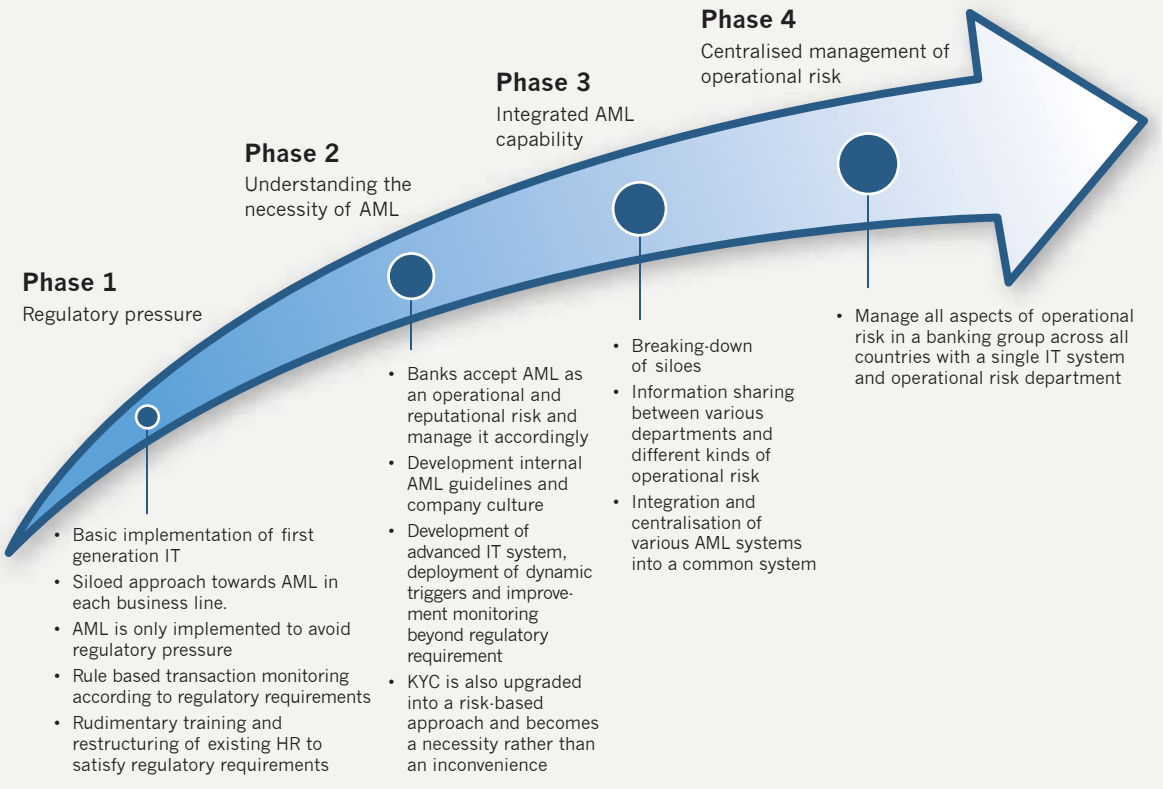
According to a foreign bank, the main focus of AML implementation in China is twofold: "The first is customer identification when customers open an account. The second is when customers transactions are classified as suspicious. We have customer ID verification system, framework processes in place, and risk management processes in place."

Large value and suspicious transactions

Several commercial banks stated that most AML jobs are guided by regulations and administrative rules issued by the Chinese government and PBOC. No internal rules and guidelines have been put in place. This impedes the quality of AML efforts, as banks usually do not supervise and robustly audit the successful implementation of AML.

The Chinese regulator obliges banks to report large value and suspicious transactions to the Anti-money Laundering Monitor and Analysis Centre of China (CAMLMAC). Large value transactions are generally stored centrally in the branch back-office on a city or above level. Large value reports can be automatically extracted directly from the data centre and transmitted to the CAMLMAC.

Figure 2.1
Maturity development of AML in banks



Source: Asian Banker Research

"We have our own bankwide risk management department and it is in charge of the whole bank's risk control issues."

Senior Executive of a Joint-Stock Commercial Bank

For an effective combating of money laundering, banks need to take AML away from the frontline. Suspicious transactions are still mainly identified by frontline staff in local branches who perform AML on top of their regular tasks. In most Chinese banks, the identification standards are not quantitative and depend on a combination of system filtration, staff's logical reasoning and sensitive recognition. Since information from suspicious transactions needs to be condensed, filtered, complemented, categorised and reported throughout a comprehensive hierarchy from the operational level via branch back-offices on higher levels to headquarters and finally the regulator, the identification and response can take weeks. "Most financial institutions have to focus on real-time detection, rather than post-supervision, which results in the fact that detection is mostly limited to deposits and withdrawals over the counter", says the AML Bureau.

In the case of a suspicious transaction, banks often cannot determine the reason for the transaction, whether it is money laundering, fraud or sanctions. The bank only knows that there has been an unusual transaction and files a suspicious transaction report. As doubtful transactions happen frequently, banks with low analytical capabilities tend to ignore AML rules altogether.

The people factor is aggravated by the high attrition rate of counter staff, quitting the bank or being transferred internally. Senior AML experts are usually rare, and not all staff assigned to AML duties receives proper training.

IT solutions and operational structure

A number of Chinese banks are currently taking the threshold to Phase 2 and target centralised AML infrastructures. However data quality and core banking integration issues remain a challenge.

Chinese banks have been investing in IT software and process modification when urged by regulators. Generally most banks opt for cheap and basic off-the-shelf systems which only satisfy regulatory requirements and put the regulator at ease. We have observed that most IT systems have been implemented in a hurry and without much interest in quality or sustainability. First generation low-tech rule-based monitoring tools, which focus on detecting and flagging but not on alert accuracy, do not assure comprehensive suspicious transactions reporting. These rules are often stiff and based on regulator demands, and are thus inflexible and not suitable for a fast paced AML environment. Changes in extracting rules would even require a re-coding of the detection systems. It is difficult to scale up these first generation IT systems to keep up with the rapidly changing requirements.

Another major roadblock comes from rules-based systems triggering too many false positives, overwhelming compliance staff. Rules-based systems drive volume and not quality. The increased volume of work items may diminish the credibility and energy of AML monitoring staff, distracting them from their primary responsibilities and preventing the department from meeting AML obligations.

Manual documentation is adding to the woes for cash transactions. AML systems are connected to retail debt systems, personal credit systems, and credit card systems. While this allows the tracking of all electronic transactions, cash transactions, which make up for 65% of Chinese banks total transactions, cannot be monitored automatically. Employees have to add the relevant data manually, which not only increases employees' work but also cannot guarantee data quality.

With the spread of e-banking, the frontline-based suspicious transaction monitoring system becomes even more insufficient, as bank staff has less face-to-face contact with customers. Criminals increasingly use the internet to participate in money laundering activities which adds another layer of difficulty for banks to identify them.

There are also some Asia-specific concerns, which make automation in Asian countries more difficult. A particular problem for China is the romanisation of Chinese characters for payment transactions, such as SWIFT. There are too many possibilities of translating a Chinese character into Latin characters. Moreover, the software has to struggle with the different order of first and last names, and English pseudonyms for Chinese names as well as random English given names.

Other cultures have different name conventions. For example in countries with a Muslim population names are written differently from country to country, and a popular name like "Mohammed" can be written in more than 50 different ways. In Malaysia and Indonesia, people often do not use surnames, which are usually simply the father's given name, and would mainly use their own given names alone for identification instead.

Many Asian countries have problems with the limited space in payment transaction forms, which leads to truncated names. These hinder name-matching capabilities with international black lists, politically exposed persons (PEP) profiles, terrorists, etc.

International banks usually do not deploy China-specific systems, but work closely with the regulator to meet these requirements. Usually they make use of the systems they already have in place in their home market.

Other stumbling blocks are organisational deficits. Some banks do not operate a specialised AML department, and in some cases there is not even a supervisory body in the bank, resulting in loose AML organisation structures, unclear responsibilities, and limited information sharing and cooperation between departments and inefficient AML patterns. This negatively affects timely technical support and creates an inability to re-allocate manpower to urgent priorities, the moment such re-allocations are called for. Large-scale money laundering involving several departments are much harder to detect.

Know Your Customer and Customer Due Diligence

The KYC process is a continuous one which constantly requires banks to update and refine information and standards. In China, regions differ largely in the known money laundering practices. Part of the due diligence process consists in defining regional high attention profiles and increasing vigilance to particular practices and target groups. As China is a large and heterogeneous country, AML requirements vary from bank to bank, and from region to region.

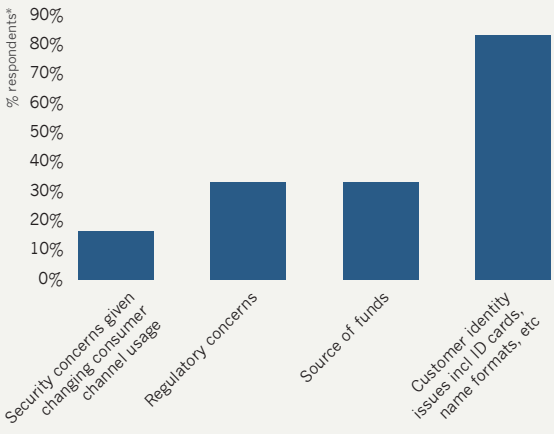
A major challenge in China, as stated by a foreign bank, is the verification of IDs, because there are so many people in China with the same name. Moreover, there are a lot of people in bigger cities who use counterfeit ID documents.

Banks also mention customers who refuse to offer necessary information. Financial institutions are obliged to collect sensitive information such as customer income and expenses. When asked these questions, customers sometimes refuse to give answers or just offer wrong information. A variety of banks have expressed problems in collecting correct and effective data.

The use of PEP profiles remains moderate in China, whereas in other countries in Asia the potential risk from those persons is incorporated in their risk profiles. The reason for this is incomplete information from Public Security Bureau, the PBOC or the social security department, and a lack of independent sources of information in China. Several commercial banks also stated the problem that public agencies such as the Industrial and Commercial Bureau do not or cannot share information freely.

Fragmentary reporting to CAMLMAC based on poor legacy customer records in the banks and un-

Figure 2.2
Challenges banks currently face in running AML programmes*



Source: Asian Banker Research

** please select up to three options*

available mandatory information also affect the efficiency of transaction monitoring and analysis. Despite checks by The PBOC, the willingness of banks to deliver useful information seems to be limited. Reports often contain wrong information and data redundancy, as some commercial banks do not pay much attention to AML procedures.

The cost of AML and Reputation

The predominant feedback of commercial banks in China was that they regard AML mainly either as a means of risk management, as a waste of time and resources, or as a major cost driver. Some even perceive it as negatively affecting profits as it scares away customers due to more complicated and comprehensive KYC procedures, and because clients are afraid of a softening of bank secrecy. Moreover, rigid AML specifications have the potential to limit business opportunities. Thus AML remains a non-issue for most Chinese banks, unless they go international.

Only a few Chinese banks take AML and the regulator very seriously, in particularly those who operate internationally. "The largest challenge is the conflict of interest between the bank and the regulator. For example, often when you believe that a person is involved in money laundering activities and you refuse to provide services to him, you lose some business such as profits from transaction settlement, commission, etc. But, frankly speaking, our attitude is to always view compliance as the highest mission in life. We are very determined here." says the risk executive of a large Chinese commercial bank.

Reputational damage and fines are still not seen as a serious concern by most Chinese banks. But things are slowly changing, and reputational risk is gaining in importance. "Failure to report suspicious transactions will enhance our compliance risk, will sometimes influence our reputation and will eventually create a commercial risk", said a manager from a Chinese commercial bank.

For internationally active Chinese banks, the risks from AML and CTF non-compliance are more immediate. Not only are the fines higher, as seen in US sanction violations over the last years. Some major banking groups, such as ANZ, UBS, Lloyds TSB and ABN AMRO had to learn about the painful consequences the hard way, as they have all been fined by US authorities with the highest fine of $ 350 million. But Asian banks have also been targeted by US enforcement authorities for trading with undesirable partners: Banco Delta Asia from Macau has been censured for trading with North Korea, and Malaysian First East Export Bank has been specifically identified as a subsidiary of Iranian Bank Mellat by the US Department of Treasury. The reputational damage from such negative publicity in the media and the association with organised crime, corruption, terrorist financing and sanctioned regimes also threatens to tarnish brand perception. One international Chinese bank mentioned it is eager to comply with AML regulation in an effort to avoid negative publicity and to avoid causing foreign regulators to take a closer look at the bank's business abroad.

Current organisational approaches to AML management

We distinguish between two general approaches to manage AML in financial institutions. On the one hand, banks organise the compliance in silos with more or less coordination from a central compliance/operational risk department. On the other hand, we see a development towards the integration of risk management into the existing IT and process architecture with a trend towards centralisation of risk management to a specific department, assuring the compliance and risk management of the whole bank.

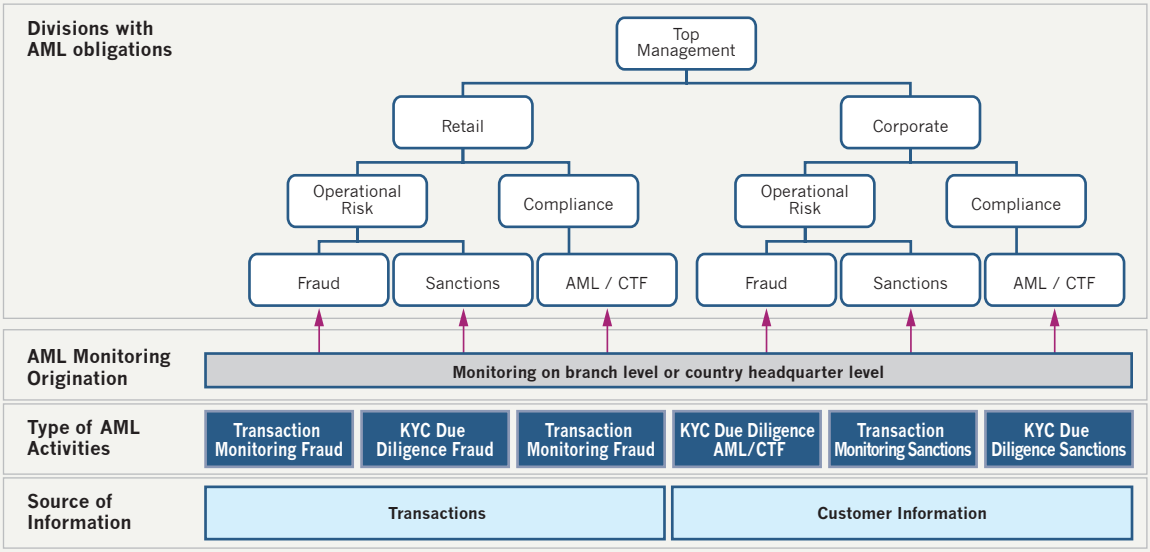
Siloed approach

The first approach is a logical first step for banks, which are forced to quickly adapt to new regulations, without a deeper awareness of the seriousness of the matter. Siloed approaches are more easily achievable, as the general structure already exists and the bank only adds some people, processes and IT. This is common in emerging markets like China, where the banks started AML from the stand under external pressure by regulators, with rather fuzzy standards and definitions.

In the beginning, the cost factor also comes into play as local basic IT is cheaply available and existing employees are only rudimentarily trained to take over new responsibilities. Within the silos, each risk is dealt with individually. There will be an AML surveillance system, which reports to the compliance or legal department and controls the channels. The fraud department, which is located in another department (like corporate security, audit or in operational risk) will solely deal with fraud. There will be another system checking sanctions in transaction banking, operated by the operations department. These structures are replicated across the business lines, such as retail, cards, corporate, as well as across various countries. Usually, information is not shared between the various departments, or at least not done so in a timely matter. As result of the silo structure, the information stays in the silo and even if the name occurs in several touchpoints within the organisation, the banks are not able to react efficiently.

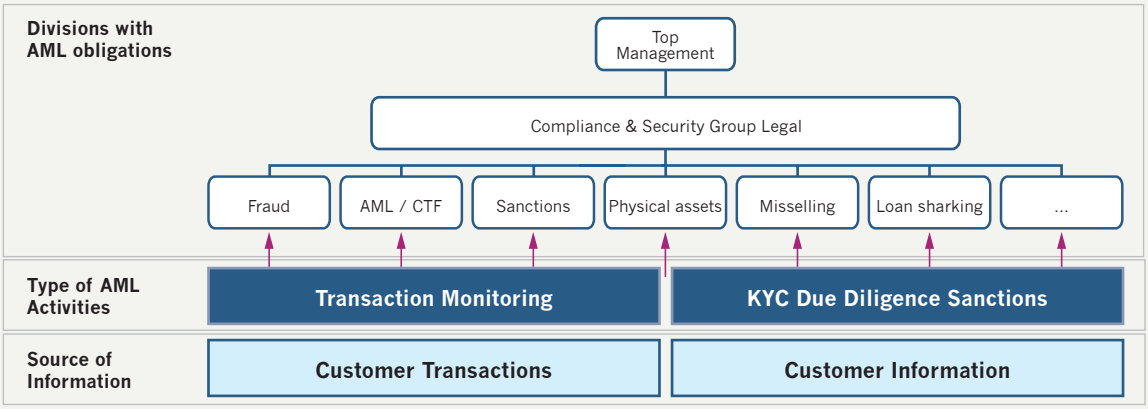
Further regulatory requirements, rapid change of money laundering techniques and the bank's inability to manage those risks efficiently makes further investments into processes and IT necessary. Because of existing legacy systems, banks continue to add on to their current IT architectures and try to adjust processes, which usually results in the creation of a central department to at least coordinate the fight against operational risks. Due to the lack of integration, information sharing remains difficult and complex. The KYC or Customer Identification Program (CIP) system is usually not integrated with a transaction monitoring system, so high-risk entities might not receive adequate scrutiny. Sparse information about a potentially suspicious event or party can lead to longer and more error-prone investigations. Alert notifications often have to be distributed manually and might be overlooked and misrouted.

Figure 3.1
Financial Crime Risk - Siloed Approach



Source: Asian Banker Research

Figure 3.2
Financial Crime Risk – Integrated Approach



Source: Asian Banker Research

A Chinese commercial bank describes its organisational structure as follows: "We have our own bank-wide risk management department and it is in charge of the whole bank's risk control issues including AML. We, as a business department, will need to coordinate with them from time to time, in order to discover any abnormal situation and irregular cash flows in the accounts. For retail banking specifically, we are detecting the irregularity of cash flows in our customers' accounts on an individual basis. If we find anything unusual, we need to inform the operation department which will pass to and solve the problem together with the risk department."

Integrated approach

The integrated solution is mainly found in advanced banks, such as a few local banks in China, and international banks like Standard Chartered. As these systems usually work bank-wide, these banks also take the know-how to their subsidiaries across Asia including China. All operational risks are managed by one department throughout the whole bank across all countries. This department can leverage fully on comprehensive data from the various financial crime risks, as well as KYC and general customer information from the CRM system. With the integration into the core banking system, automatic blocks on positive identification of blacklisted persons are possible and limit delays and human mistakes. This also allows top-down messaging on the basis of the operating system, so that messages cannot be ignored or overlooked.

Advanced analytical and monitoring software helps to achieve greater efficiency with lower manpower. As all operational risk are managed by the same department, this allows comprehensive assessment and understanding of suspicious transactions and rapid reaction according to its risk level.

Despite high implementation costs, integrated systems achieve cost efficiencies in operation, as staffing can be reduced. For example, a leading Southeast Asian commercial bank stated it reduced operational risk staff since the implementation of its AML architecture by almost 20%, despite an increase in assets and market presence across Asia.

The difficulty in integrating AML technology with all other source systems derives from the various formats and rules used in these systems. Data has to be standardised from the source systems. It helps to develop a pipe, so the rules engine can use data.

"One of the greatest risks is to manage operational risk in silos. Most banks in the world still monitor operational risk without cooperation and information sharing across departments."

Risk executive of a Singaporean bank

What banks do to overcome pain points

Large value and suspicious transactions

In order to strengthen monitoring capabilities, Chinese banks should expand the scope of transactions they are monitoring and define clear criteria on what is a suspicious transaction. Banks have to go beyond regulatory requirements and implement internal guidelines and standards.

As a local best practice example, one Chinese bank said it deploys a system that monitors the transactions of customers and correspondent parties. Suspicious transactions are analysed and if they cannot be validated, a customer manager will try to find out the purpose of the transaction. If this does not work either, the transaction will be transferred to the compliance department to investigate the customer. In this case, account information of the last six months will be checked together with public information to see whether there is suspicious AML activity. If the suspicion is substantiated, the customer risk will be adjusted.

The same bank double-checks the information of 1,500,000 customers with the online system from the PBOC. For companies, profiles and information on the legal representatives will be checked. Therefore the bank developed a system internally to report important suspicious activities.

If customers change their trading categories, the bank is able to track this change with another additional system.

IT solutions

Improved IT solutions bear high potential in AML capabilities. Employees can be relieved from complicated filtering, identification and reporting processes, which will greatly improve work efficiency and quality.

One Chinese commercial bank established an electronic system, which on an ongoing basis con-

trols all persons, firms and organizations mentioned on any list of known fraudsters, terrorists or money launderers. The system also monitors and reports large cash and suspicious transactions.

Leading-edge surveillance systems have useful tools, such as real-time watchlist filtering capability with fuzzy logic. This helps name matching, as a variety of names can be checked. When a payment instruction goes through a payment gateway, the system checks every single word in the instruction with a sanction list.

Some banks have already started centralising AML-related tasks and data and builds data models that include a broad range of product types, channels, entities and non-monetary events. Optimally, the alert-generation process should monitor multiple risk factors with a single pass through the data – even for very large databases.

Know Your Customer and Customer Due Diligence

In China, regions differ largely in the known money laundering practices and therefore require a refinement of regional high attention profiles, an increased vigilance to particular practices and target groups as part of due diligence.

Information sharing among banks, regulators and other official data sources like credit data, but also foreign PEP profiles, has to be improved; data quality and communication channels have to be cleaned and streamlined.

With a risk-based approach to AML, banks can optimise their efforts by watching high risk customers closely and can spend less time and effort on low risk customers. A variety of factors have to be taken into account, such as the type of customer or business, product and expected account activity. Risk-based customer acceptance procedures need to be consistent across all branches. They require banks to ask a set of questions and include rudimentary database research to determine the risk level of customer. Taking the risk of higher levels should be decided by higher ranks or even a committee, involving the senior executives.

Risk profiling can help to cope with KYC risk. The three tier risk model – classifying customer profiles with high, medium and low risk – is the most common. The actual idea behind the model is basic, but the implementation is tricky, as the risk profile has to be strict. Capable mechanisms and people building these mechanisms are inevitable for success. Risk profiles are based on a variety of indicators, which for individuals usually include place of residence, country of origin, citizenship, source of wealth, occupation, and countries to and from which transactions are to be made. For legal persons they should contain the location of business, country in which the business is incorporated, nature of business, beneficial owners of the business, directors, countries from which transactions are made and entities with which the transactions are affected. These indicators derive a blended score. The better integrated such risk models are in the monitoring and decision making process, the more effective the risk management. Automated data updating and recalculation or risk scores keeps the profiles accurate and up-to-date.

Some helpful indices for country risk are the OECD non-cooperating tax havens list, FATF non-cooperating countries, Corruption Perception Index, etc. Such indices are comprehensively researched and do not have a high risk of being politically motivated, unlike country black lists.

Desk research on cooperate background and individuals, news releases and PEP profiles from information sources such as Factiva, combined with internal intelligence systems, internal rating, negative lists and law enforcement reports, deliver individual information. Internal databases have to be constantly updated and checked.

A Singaporean bank collected business intelligence and indexed the data in a central intelligence platform, which is linked to the transaction surveillance system and core banking platform. This allows the bank to react quickly if a customer is identified positively on a black list. In this case, the desired action can either be blocked or associated with a higher risk profile and closely monitored.

Company culture

In order to drive compliance, a financial institution requires substantial understanding and support from top management. Investments into the implementation of IT processes and employee attitude require explicit and unequivocal support from the

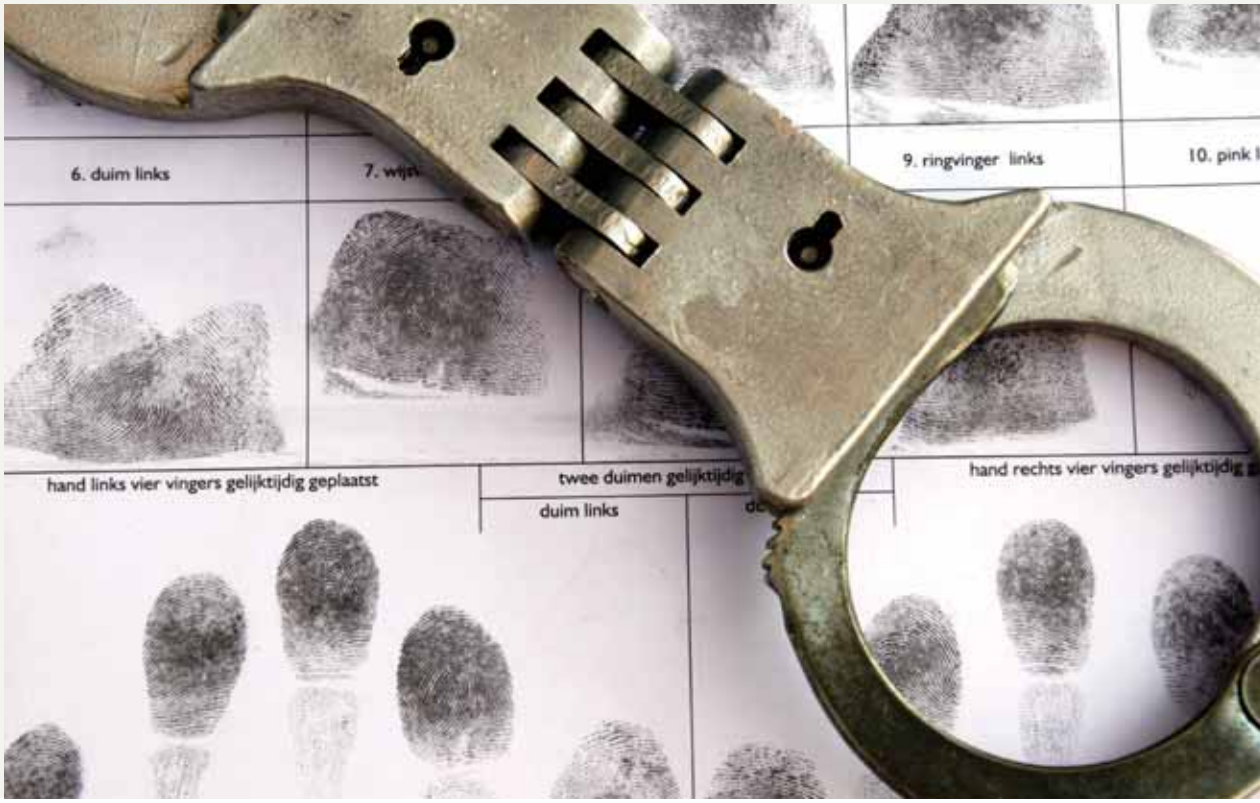
senior management. An interviewee who has been in charge of AML in several banks described the resilience of a variety of banks to engage a serious new corporate policy towards AML. The reasons for this are the enormous cost and restructuring requirements needed to achieve full AML capability in a major bank, and the complex problems in dealing with legacy systems, internal restructuring, insufficient understanding of needs and benefits. In a best practice example, the whole hierarchy of a bank from the CEO and chairman downwards conveys the message and importance of AML to all employees.

After creating a culture of a highly involved senior management, the development of a code of conduct for all employees of the bank is the next step. Only a few banks publish such codes publicly, stating key obligations for staff and conveying the importance of the matter. This allows customers to access the material and detect and report non-compliance.

This also involves solid escalation mechanisms, which require the full understanding of employees, definite rules and escalation channels, a system to distribute messages and warnings, but also needs to deal with the issue of whistle-blowing while building incentives for escalation. It is vital to develop a system that leaves no space for hesitation and disorientation. A single drop-in centre for all issues involving operational risk and an information sharing system, which makes sure that all the people involved in dealing with AML get the information they need, is necessary.

In emerging markets like China, we realised that for a majority of banks branches are still the main location for combating money laundering. These banks believe that branch employees are in a better position to detect money laundering, as they understand operations and customers better. On the other hand, there is a growing number of banks in China who perform centralised monitoring in the headquarters. In any way, comprehensive and continuous training is a necessity for the success of AML.

An enterprise risk approach helps to manage risk more efficiently and also to bring down AML-related cost. Among the basic steps to achieve an enterprise-wide integration is the consolidation of AML into one compliance department and the integration of all systems on one technology platform. Furthermore, it is beneficial to combine AML and anti-fraud efforts. Finally, a central case management system brings together the output from disparate systems.



Critical elements of a robust AML programme and best practice

When asked what makes a critical AML regime, interviewees noted that technology still plays a major role for banks. But there is a rising understanding that it takes more than a good IT infrastructure to effectively combat money laundering. Only a few banks in China have fully embraced this fact.

A senior executive of a commercial bank says, "AML should be conducted on a daily basis, not just for several days. The system can identify some suspicious transactions every day, and automatically downloads transaction data. So I believe that real-time monitoring and complete records of client's transaction data are the most important elements."

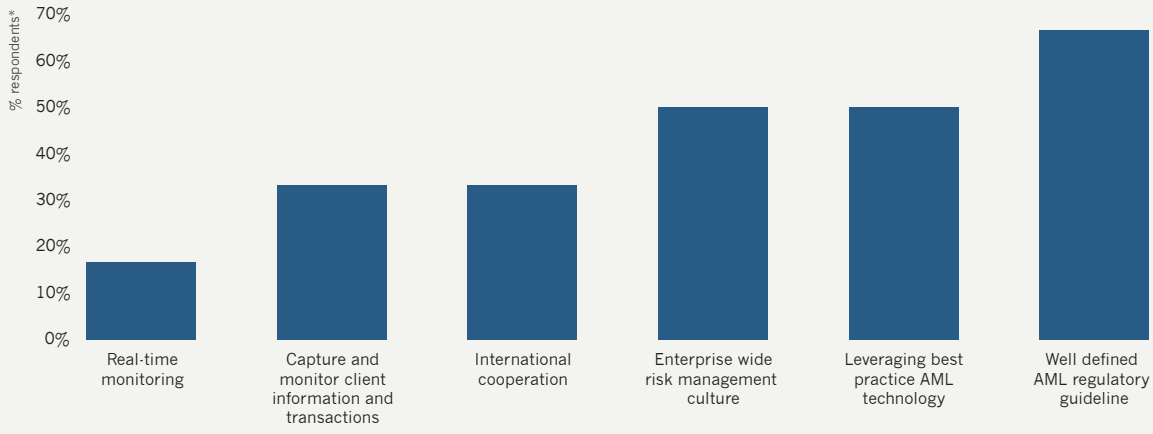
The vice president of a big four bank believes that Chinese banks need to have in-depth communication and conversation with peers in other countries to prevent financial crimes. He emphasises the need of Chinese banks to better cooperate and share information with international organizations to learn more about the situation in China.

According to another Chinese megabank, a robust AML programme is based on four factors. The first is building a customer information database system to keep records of customers' identity. The second is building a more robust large-amount and suspicious transactions reporting system that can be used by banks and non-bank institutions. The third is strengthening the internal monitoring system and establishing a mechanism to evaluate staff's integration, work experience, and financial records, as well as providing continuous training programs for employees and strengthening independent auditing. The last is coordinating with international AML organisations.

> "In my opinion, the most important criterion gauging the robustness of an AML programme is the filtering rate. I am not saying a too high or low rate is good, but the accuracy of the filtering/ screening rate is important."
>
> *Senior Executive of a Joint-Stock Commercial Bank*

As a best practice example in the region, we regard DBS' fight against money laundering. Starting with the objective of managing all kinds of operational risk with one system in one department, the bank built a groundbreaking AML infrastructure across all channels, products and countries.

Figure 4.1
Critical elements representative of a robust AML programme*



Source: Asian Banker Research

** please select up to three options*

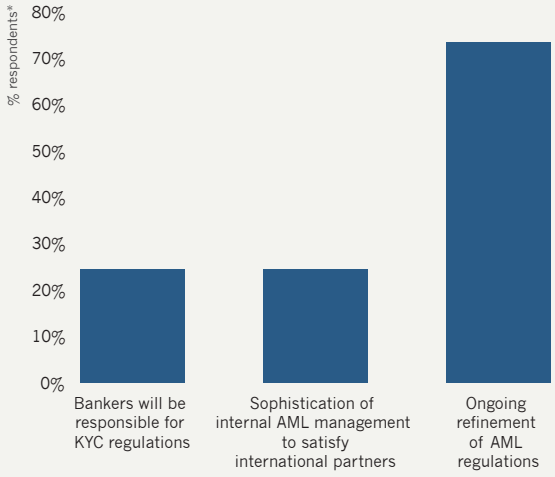
Future regulatory developments

Most banks expect from the regulator a further strengthening of regulation and also stricter enforcement of the existing regulation.

"Without a doubt regulations will be much stricter than before, especially under current market conditions. And even when the crisis passes its worst, I don't project there will be a sudden ease in the regulators' attitude. It's a good time for them to rebuild the discipline of the market", says a Chinese commercial banker.

Figure 5.1

Expectations of future developments in AML regulatory regime*



Source: Asian Banker Research

** please select all those that apply*

A big four bank expects a perfecting of regulatory guidelines in the near future. This includes the establishment of a policy that makes the reporting of suspicious transactions mandatory. It is also expected that banks will have to pay closer attention to capital from countries, where AML regulations are not enforced or are incomplete.

However some banks still hope that they will somehow manage to avoid major changes in their behaviour and that the regulator might exempt financial institutions from responsibilities, when their behaviour is based on bona fide and report suspicious transitions to authorities.

For the moment, transaction monitoring in China focuses mainly on large transactions. Having achieved basic AML capabilities, the regulator might urge banks to take further steps to improve reporting standards, customer due diligence, monitoring and analytical capabilities. KYC requirements might be expanded to involve third parties in transactions and customer's source of funds.

Banking secrecy will also be debated and might result in changes in offshore banking models.

In order to raise the awareness and deterrence effect of non-compliance, the Chinese government will have to raise and strictly enforce fines and penalties. This may even include prison sentences for individuals for serious violations. Personal liabilities of senior bankers are also considered in Hong Kong and it is to be expected that other Asian countries will follow.

For further information, please contact:

Temenos Singapore
61 Robinson Road
#20-01 Robinson Centre
Singapore 068893

Reid Warren
Tel: (65) 6536 6722 / (65) 6232 3216
Fax: (65) 6538 0818
Email: rwarren@temenos.com

www.temenos.com

The Asian Banker
10 Hoe Chiang Road
#14-06 Keppel Tower
Singapore 089315

Chris Kapfer, Associate Director, Research
Tel: (65) 6236 6520
Fax: (65) 6236 6530
Email: ckapfer@theasianbanker.com

Thomas Zink, Research Analyst

www.theasianbanker.com