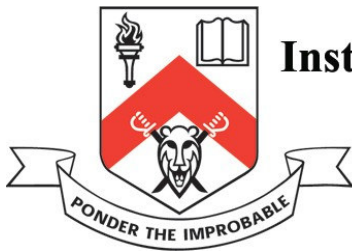


AML/CFT

– New Policy Initiatives

PRICEWATERHOUSECOOPERS 



Institute of Defence & Strategic Studies

July 2005

The Authors

Rohan Bedi, Head of AML Services, PricewaterhouseCoopers Singapore

Arabinda Acharya, Associate Research Fellow and Manager Strategic Projects,
International Centre for Political Violence and Terrorism Research, IDSS Singapore

Contents

Topic	Page
Introduction	3
Competitiveness	5
Regulatory Burden	7
Risk-based Due Diligence & Program Quality	9
Training	12
Awareness	14
Leadership - Tone at the Top	15
Independent Testing	16
Terrorist Financing	17
STR Filing	21
Feedback from FIUs	23
Guidance from Supervisors	25
Technology	26
Personal Accountability and Professionalism	28
Public Awareness	29
Acknowledgements	30

Introduction

The PwC-IDSS thought leadership series is being launched with this paper on possible new supervisory policy initiatives. Supervisory policy creates the rules for Suspicious Transaction Report (STR) filing by financial institutions (FIs) given the need for intelligence by Financial Intelligence Units (FIUs) to fight drug trafficking and other criminal activities. The objective of this paper is to engage and solicit the opinions of key industry participants on where we are globally on key Anti-money Laundering (AML)/Combating the Financing of Terrorism (CFT) issues; where we want to be; and how to get there.

The Debate Rages On

At the outset we underscore our belief that fighting crime is important for any country or society. However, as the UK Identity debate underscores, many in the industry believe that it is important for law enforcement agencies to have realistic and proportionate expectations of the information likely to be available to them. *The fact that law enforcement has ‘needs’ does not mean that meeting them should automatically become a matter of regulatory obligation or universal practice.* Nor do these needs have to be met only through the ID process.

It is now accepted that fighting crime is not just the responsibility of the authorities. FIs too have a critical role to play. What industry is debating on is – “How much can we do and how do we do this? Are we losing sight of the customer service objective? Don’t tell us that ‘Know Your Customer’ (KYC) leads to better product sales and customer service delivery – more information always helps but our clients are none too pleased with our constant burgeoning need for AML linked information”... There is evidence that AML/KYC requirements have caused much pain to individual clients including denial of service. One example is the ID debate in the UK on issues such as whether one check of identity could also back-up as a check of address. Furthermore, some jurisdictions enshrine in law (“constructive trustee” provisions) the banker’s responsibility to act promptly on his clients instructions – this exposes banks to the risk of clients suing them for damages arising from delays if reasonable cause is not shown.

The UK ID debate underscores the fact that industry has expressed strong concerns about the increased costs of AML and questioned whether their investment provides value for money. AML is one of the biggest drivers of increased compliance costs and firms are questioning whether this was leading to a competitive disadvantage for them and a cost that bore little relation to the benefits achieved.

Our Methodology

This paper is not a survey. The results are based on our views taking into account the responses to questionnaires from selected key individuals from banks, vendors and FIUs. This is in order to obtain a better understanding of what key AML interested-parties think

PwC-IDSS Thought Leadership Series

and to focus our viewpoint. The responses are based on the individuals' perceptions and views, and do not purport to represent those of their organisations. Some of the respondents have chosen not to be quoted and we list them in the acknowledgements section instead. One chose to be anonymous.

All questions on Asia are ex-Japan; questions on 'Asia (generally)' are ex-foreign banks for the banks section and ex-Hong Kong/Singapore for the FIU section.

For the purpose of this paper, we are commenting on the banking industry although many of our conclusions have wider implications.

Detailed Findings

Our paper is focussed on *high-level issues* that we consider important. It is neither intended to be super-comprehensive nor deals with micro issues.

Many of our suggested "future actions" underscore a need for a "*back to basics*" drive on issues relating to AML in Asia. The paper is also useful from a global AML perspective as it raises some key issues that go beyond Asia. Importantly, our objective is to give "renewed focus" to many key issues which are currently unattended.

We comment on the following areas in three sections each – Observation, Need and Future Action.

1. Competitiveness
2. Regulatory Burden
3. Risk-based Due Diligence & Program Quality
4. Training
5. Awareness
6. Leadership - Tone at the Top
7. Independent Testing
8. Terrorist Financing
9. STR Filing
10. Feedback from FIUs
11. Guidance from Supervisors
12. Technology
13. Personal Accountability and Professionalism
14. Public Awareness

1. Competitiveness

Observation

This is an issue of some concern to supervisors who wonder whether AML practices are in fact anti-competitive i.e. if a country is a leader rather than trailing along, would this be harmful to its' business? Intuitively the answer seems that this is in fact the case, but interestingly this is not a mainstream industry opinion. AML practices are regarded as part of normal due diligence practices and are not viewed as reducing competitiveness; in fact the market may be divided as many believe that it may in fact increase competitiveness.

Our view is that in the longer term, good AML practices will enhance competitiveness. At the same time, the importance of a “level playing field” in the shorter term must be underscored. We agree with *Srinivas Vishnubhatla*, Vice President Business Development, IntegraScreen (America) Inc - that AML practices can be anti-competitive in the shorter term if they are implemented unequally across countries and may lead to movements of monies from one centre to another – both by genuine clients and by launderers. Private banking clients for example, want privacy and convenience – if these get endangered in any country, they will move their money to another financial centre. Hence, AML regulations are in practice implemented in a “neck by neck” manner in many financial centres to prevent a loss of competitiveness i.e. they prefer to do what their peers are doing – no more, and perhaps less in certain instances (such as the issue of tax evasion).

The Financial Action Task Force’s (FATF) identification of new Non-Cooperative Countries and Territories (NCCT) was an important exercise that was stopped. This exercise has in the past not adequately covered higher-risk countries in Asia and in many cases being removed from the NCCT list has not been meaningful as implementation of the AML rules has not been up to the mark. In theory, a country gets removed from the NCCT list when its AML regulations are in place *and* its implementation is up to the mark – in practice, on-ground implementation continues to be weak even after being taken off the NCCT list.

Need

The lack of effective on-ground implementation is an issue that launderers exploit. A launderer would rather launder his/her monies through a country that is not on the FATF NCCT list and that has poor on-ground implementation of AML regulations. To banks dealing with these countries, the risks may not be readily transparent in the absence of branch operations in these countries or a developed money laundering risk monitoring system. There is thus a need to identify such countries, which the current FATF assessment processes review only at a very macro level and in many cases give a clean chit to.

Future Action

- *Effectiveness of Implementation – Enhanced FSAP Methodology Needed*

PwC-IDSS Thought Leadership Series

We believe that quasi-regulators such as the FATF can adopt a more meaningful approach to the whole issue of measuring “effectiveness” of AML implementation on-ground in countries.

The current IMF-World-Bank-FATF Financial Sector Assessment Program (FSAP) AML/CFT methodology may not be adequate as the reviews tend to be very high level and miss critical gaps in on-ground implementation. For example, broker-dealer AML regulations may exist but in practice, KYC practices may not be up to the mark. Organisational AML culture may also be completely lacking. Another key-indicator could be the extent to which AML technology is adopted in a country – lack of adoption may suggest a poor implementation status in today’s AML context.

Specifically, the FSAP process needs to be enhanced through working with independent audit firms to bring in a more micro audit-and-review methodology which uses a blend of traditional assurance testing with a broader AML expert-based review process. This process can be focussed on randomly selected banks/FIs in different categories. The UK Financial Services Authority (FSA) has as part of its ‘toolkit’ a possible requirement for a “*skilled person*” report which can be used for a number of purposes including “Diagnostic checks” i.e. to identify, assess and measure risks. This is the sort of enhancement that the FSAP process needs. This is in addition to other controls already in place i.e. internal audit and independent supervisor AML inspections for perceived higher-risk banks.

We believe that a better assessment of “effectiveness” of implementation of AML regulations will contribute in a meaningful way to a *level playing field* addressing concerns of countries taking the lead in AML practices.

- *Implementation Focus – New OILC Country List*

Furthermore, rather than talking about a NCCT list which implies non-cooperation, we believe that the above enhanced FSAP methodology should be tied in with a possible new FATF exercise of “On-ground Implementation Lacking Countries (OILC)” list. The focus should now be squarely on actual “*on-ground implementation*” rather than “perceived” implementation. For this exercise to be meaningful and credible, FATF member countries that have poor on-ground implementation should also be highlighted. Furthermore, the whole idea is to emphasize risk rather than use sanctions to whip these countries. Being on the OILC list would itself generate sufficient pressure for countries to act especially since most of these would have AML/CFT regulations and are mostly cooperative ie, sanctions are not needed.

2. Regulatory Burden

Observation

AML is one of the biggest drivers of increased compliance costs in the West and certainly smaller banks are beginning to feel the pressure and complain about this new regulatory burden. The banking associations have started to take up their grievances with supervisors for clearer rules, more supporting information, and paperwork reduction wherever possible.

There is a small yet growing school of thought that believes that governments have overreacted owing to global pressures and that crime must be fought directly rather than forcing FIs to join in the fight. This school of thought believes that the AML/CFT exercise is a case of misplaced energies.

However, industry generally believes that governments are justified in their approach as the threat of money laundering and terrorist financing is very real i.e. it is not out of proportion and is not just based on the tragic events of September 11, 2001. *Peter Hazlewood*, Vice-President for International AML compliance at JPMorgan Chase specifies that “Governments are justified in their approach but have struggled with the correct area of focus. They should focus more on quality programs and less on quantity of coverage.” We agree with Peter and will consider specific issues on AML Program quality separately.

Furthermore, when controls developed in Western countries are applied in an Asia-Pacific retail banking environment (for example, in South Asia), the higher volumes of transactions may make many controls little more than a paperwork exercise. For example, where line managers in retail banks have dual signing requirements for transaction approval above a certain value, in practice this will degenerate in many bank branches into a hindsight review with a lot of ‘*blind signing*’ happening on the ground.

Need

The issue of regulatory burden must be seen in the light of the fact that regulations have tended to be cumulative i.e. a little more every couple of years. In the US the American Bankers Association carries on an ongoing exercise of filing comments solicited by the US FinCEN (the FIU) on paperwork rationalization under the Paperwork Reduction Act 1996 to eliminate regulatory requirements that are outdated, unnecessary or unduly burdensome. We believe that a similar role can be adopted by supervisory and banking associations in Asia as well, under the theme of paperwork reduction.

Our observation for Asia is that many larger institutions seem to be the focus of supervisory attention (especially if facing regulatory action in some other parts of the world), whereas the smaller one branch operations (that in many cases have insufficient AML systems) get away with little or no comments. Furthermore, foreign banks are the focus of attention whereas national institutions that may have poorer AML systems often get away with little or no comments. *We believe that this is iniquitous and needs to be rectified.*

With reference to the ‘*blind signing*’ problem, this situation does not do away with the need for such controls. Rather it underscores the fact that in high volume scenarios a strong process is needed for independent risk assessment of transactions that retail banking line management may not be in a practical position to satisfactorily provide on an ongoing basis.

Future Action

- The goal of paperwork reduction is best accomplished when government-industry partnerships emphasize quality over quantity. This could include for example, questioning the value of a CTR threshold of USD 10,000 in the US, versus the quality of information it provides for intelligence purposes; or adopting online STR filing with auto-responses for submissions with filing reference numbers. Initiatives such as these can go a long way to eliminate manual work at banks in very many forms.

Moving to electronic transactions and electronic signatures can also reduce transaction costs for FIUs owing to faster access to the data and easier data analysis. Furthermore, reengineering the work process associated with the transaction around the new electronic format can also give rise to other efficiencies within the FIU.

- Supervisory focus in AML inspections needs to be on weak areas in banks irrespective of whether the institution has the spotlight on them owing to regulatory actions elsewhere, irrespective of size and irrespective of whether it is a national institution or not. Money launderers will exploit the weakest link in the chain.
- In high volume retail banking scenarios a strong process is needed for independent risk assessment of transactions, which banks should focus on. This can be in the form of a strong internal audit function in the branch cross-checking transactions on a daily basis or centralized monitoring of transactions albeit the former is a preferred option.

3. Risk-based Due Diligence & Program Quality

Observation

Jay Jhaveri, Director Asia for World-Check states “The move towards risk-based due diligence demonstrates the move towards thinking out of the box in risk matters” – we can’t agree more with him on this definition and urge banks to move away from “tick-box” compliance approaches.

The importance of a risk-based approach in a customer service industry must be underscored. Put simply it helps a bank to prevent bad customer service through asking unnecessary questions when all the facts taken together clearly identify a lower risk scenario. The more traditional viewpoint is that risk-based due diligence helps to conserve a bank’s resources – in the business units undertaking the KYC process, in the approach of Compliance, and in the focus of Internal Audit on key risk areas. Interestingly, the importance of risk-based due diligence for customer service is not recognized by many in the compliance function. Having said this, most compliance staff, are ready to work proactively with business units to waive operating requirements in low-risk scenarios. Very few believe that this is the prerogative of compliance alone and there is also a growing school of thought that branch/unit managers should be empowered to do this based on judicious documented reasons.

In a longer term view, we tend to agree with this new school of thought as there is a wider need for business units to take responsibility for risk assessment which should come about (in theory at least) once the onus is put on them for ‘judicious waivers’ for low-risk cases. However, internal audit would have to ensure that this is in fact a judicious decision making process as would training need to be risk-based to ensure the development of this capability. In the absence of both these capabilities (widely seen by us) we believe that for now it is better to be conservative and for compliance/ branch/unit managers to work in tandem.

Key to the whole issue of AML Program quality is whether a risk-based approach is adopted by banks including the adoption of technology for KYC black/hot-list checking and for trend monitoring where considered essential, for example in an online business or a high-volume scenario.

Enhanced Due Diligence (EDD) is another grey area where most banks in Asia (generally) just do due diligence with an additional layer of management control. EDD requires independent data-sources in addition to independent layers of review – this point is missed out by many banks. Furthermore, a lot of public domain information which is important for the EDD process is non-digital.

A KYC vendor in the EDD space in Private banking/ Trade Finance whose clients spend dominantly on credit linked cases states “In the work we have done so far for our clients we have discovered that the people we screen out in our EDD are not necessarily “terrorists” or even are covered by the predicate crimes defined by the FATF. In most cases they would

PwC-IDSS Thought Leadership Series

count as pure “credit” risk to the banks”. This underscores the potential payback from a risk-based due diligence process. Other feedback suggests that using third parties for EDD for large value deposits/investments can also lead to good quality information on reputation risk even if no clear money laundering scam is uncovered. Furthermore, a regular review of high-risk customers is critical as ownership and management changes also have to be monitored i.e. a client who is good today may not be good tomorrow.

Need

Our experience with banks in Asia is that because a risk-based focus is yet to come into supervisory AML rules in many countries, this approach is not as widely adopted by banks. For example, many banks have not started flagging the accounts of higher-risk businesses. In larger financial centres, many banks are aware of these businesses and some have taken action, while others will take action in 2005-06. In other countries, many banks may not even be aware of these businesses.

Technology adoption in Asia is also nascent as it is expensive, no AML rules explicitly require this and supervisors are not pressing as strongly as they should on this issue. Some amount of spending on KYC data-bases has commenced but often with single user licenses. Where the bank has US/UK parentage a names recognition technology may also be used as part of a broader transactions monitoring program.

Know Your Employee is another weak area in Asia where banks have poor controls – both in pre-hiring screening and ongoing KYE controls. Interestingly, some in industry believe that KYE awareness is increasing in Asia. We believe that such awareness in Asia is not matched by any real action – for example, many private banks continue to hire staff with their client relationships and then treat both the new hires and their coveted relationships as if they have been with the bank for years. Some new bank branches literally have a “founder status” for some of the more senior private bankers they have hired. This linkage of compliance approaches to business considerations is a dangerous one from an AML perspective. A Private Bank hiring a new private banker with his/her clients should treat both as new to the bank and due diligence standards should be just as rigorous as would normally be the case i.e. the processes must be undertaken and any waivers documented with proper sign-offs. There is a mistaken belief amongst Private Bankers that they ‘Know their Clients’ owing to the close personal rapport they have with them. This is a danger as personal relationships with a “*clients advocate*” culture can lead to poor compliance standards as many US Private Banks have found out. This is why the MLRO/compliance officer must be independent of business and have a strong status within the organization to allow him/her to raise issues where required. This also underscores the need for independent reviews by internal audit of higher-risk customers as part of their overall health-check of the AML program.

For Program quality, the quality of the STR filing (internal/external) is essential. The information collection and review process and the decision making must be solid. Our feel of the STR file is that this is often quite poor because neither the sources of information for

PwC-IDSS Thought Leadership Series

enhanced due diligence or the process for getting these information pieces have been defined.

EDD type information includes considering litigation/court actions, bankruptcy filings, criminal record searches, regulatory filing checks i.e. regulatory prosecutions/ sanctions. Most banks would not be in a position to get to these information sources by themselves, hence they need to use the services of third party external EDD vendors to dig out such information wherever considered necessary.

Beyond these there are numerous quality issues, for example, active involvement in the AML program by the senior management, non-suppression of STRs for business reasons, data quality especially for older higher-risk accounts etc.

Future Action

- Supervisors need to give more prescriptive guidance in their AML rules on risk/ quality linked issues especially on the role of senior management, technology/KYC adoption, higher-risk business and flagging requirements, the enhanced due diligence process - the need for a “build or buy” discipline to ensure that EDD actually happens.
- It is important to nurture the development of decision making skills for “judicious waivers” for lower risk cases by business units working in tandem with compliance units. AML training must focus on risk-based due diligence to facilitate this and specific examples of low-risk scenarios should be focused on.
- Leadership is critical – anti-financial crime is a sensitive area:
 - The MLRO/Compliance officer’s position must be staffed by a senior experienced person and organizational recognition of their role/authority ensured.
 - Ideally, the MLROs position should be separated out from the Compliance Officers position to give it the focus it needs.
 - In many jurisdictions there is an obligation to report all financial crime to the FIU. This means that a MLRO with a poor knowledge of fraud and all that goes with it will only be able to deal with the AML issues in a narrow way.
 - Salary scales need to be stepped up in Asia to reflect the importance of the position and to attract the best talent.
- Supervisors must put KYE linked rules explicitly within the AML guidance especially on pre-hiring screening practices.

4. Training

Observation

There is a broad consensus that training needs to be delivered in a blended solution between class-room training and e-learning. There is a need to use more engaging methodologies such as case-studies, role play, video and audio to build a risk-based approach. The pick-up of both e-learning and role play is higher in the West than in Asia.

Jos de Wit, former Group Compliance Officer, ING Group, Netherlands believes that e-learning is best placed to build a risk-based approach because of the consistent messages it gives, the lower cost of training large numbers of people and the opportunity to have tested training. We tend to agree that organizations need to adopt e-learning more seriously as a means of cutting longer term training costs. However, broadly we are in favour of the “blended solutions” approach as the best one for training purposes.

There is also a broad consensus that non-tested general awareness building type annual training is not sufficient and tested training is essential although the industry is divided as to whether a regulatory rule should be introduced including setting the standards for tests. Our personal view is in favour of a regulatory rule requiring accredited training including a specification of the standards for tests.

The training programs of banks in Asia differ widely. Some use blended training solutions, focus being on risk-based due diligence, detection skills, training all staff once a year. Others do not. Most banks have a focus on training their senior management differently from front-line staff. In practice their senior management attends some portion of a standardized training program. There is a general consensus which we share, that sufficient formal training time (class-room/e-learning) for staff is at least 4 hours annually provided there are no significant changes to circumstances. However, some experts believe that this may be excessive as formal training can be augmented with awareness materials through the year – “banks are commercial enterprises and must balance risk with the need to stay viable”.

Need

While there is a consensus that e-learning is good to have, banks in Asia are not actively buying AML e-learning packages. There is still a preference for the class-room based ‘regulations intensive’ training. This is because of resistance from line management especially the senior management who feel uncomfortable with e-learning.

Knowledge of the consequences of breaking the law is important although this may not help much in detection of unusual activity. For example, for a large value company current account, bank staff has to be able to look behind the corporate veil to understand who the ultimate beneficial owner is and moreover to link this with their understanding of the company ownership structure and relationship between its shareholders, directors and

PwC-IDSS Thought Leadership Series

authorized signatories, who may be third parties; and even the companies main clients. Ultimately, bank staff has to have the capability to understand the underlying money laundering scheme.

There is no clear consensus on the importance of role play in building suspicious activity detection skills. Some think it is critical, others think it is important while others think it is just good to have. *The UN have used this technique to train prosecutors in Latin America and we believe that role play is just as critical in AML as it is in customer service.* Writing out scrip's for the launderer and the banker and possible conclusion scenarios is really quite easy with the caveat that the launderer should be played by a professional trainer experienced with the scrip of the launderer. In spite of a broad consensus that Role Play is an important part of an AML training program, most banks in Asia do not use role play in their AML training.

Everyone agrees that tested training is needed. However, in practice very few banks (with some rare exceptions) actually adopt this practice.

Future Action

- Industry bodies should study the benefits of e-learning/role play for AML training and circulate guidance to banks “encouraging” them to adopt these methodologies in blended solutions with class-room training.
- Supervisors should consider adopting a regulatory rule requiring accredited training including a specification of the standards for the tests. This would of course lead to a need for specification of the broad agenda for training (which most supervisors do at present) and perhaps the number of hours of minimum training per annum.

5. Awareness

Observation

Smaller banks tend to equate training and awareness building tactics as one and the same i.e. awareness is seen as a result of training alone. Bigger US/European banks recognize the need to separate these two and recognize awareness as being the result of an 'ongoing internal marketing campaign' run by the senior management team/the board to generate top-of-mind recall on the AML issue. Awareness is also, of course, a result of training and tested training is better from an awareness generating perspective.

Most people believe that technology plays an important role in building ongoing awareness as part of a broader package. Some even believe that the role of technology is critical and should lead the AML awareness program initiatives. Technology can be used in different ways – intranet resources on AML regulations, guidance and case-studies; e-learning for example a daily 10 minute case-study; and online articles for example by tying up with a leading AML newsletter for bulk distribution of relevant articles.

Need

Key in sustaining awareness amongst line staff is to focus such efforts around issues relevant to line management. For example, AML newsletters can carry as many as 5 articles a day many of which may not be relevant to the business and some may be academic debates. Therefore, careful selection of the material being circulated will lead to broader interest and involvement. The awareness program needs to be driven by the banks senior management/the board.

Future Action

- Banks must consciously use technology to sustain ongoing awareness in addition to senior management periodically stressing the need for good business and the personal consequences for staff being negligent. Leadership of the awareness program is critical and is discussed separately.

6. Leadership - Tone at the Top

Observation

Industry generally believes that senior management in FIs in Asia (generally) appreciate their personal accountability. Some however believe that they are not sure what they should be doing to execute their responsibilities while others believe that they are actively involved in AML. There is a smaller school of thought that does not believe that senior management appreciate their role/ personal accountability in AML. *Jay Jhaveri*, Director Asia for World-Check states “Some of them believe that harsh AML/CFT procedures are an impediment to developing business”. We tend to agree with this view.

We believe that boards/senior management in FIs in Asia (generally) know what they should be doing but are not doing it. This can be judged from the low amount being spent on AML technology and AML consulting projects in Asia. AML is yet to be recognised as a specialised area that many banks may not have the internal expertise to handle. This ultimately links up to regulatory action. In the absence of penal action such as fines being imposed or public censure of banks by Asian supervisors, banks do not perceive the need to step out of their comfort zones.

Need

AML budgets are needed to ensure that adequate resources/skills can be created for AML purposes – people, technology, specialist consulting. Ongoing awareness driven by senior management/ the board needs to be focussed on.

Future Action

- Supervisors in Asia need to send a strong message on AML issues on the lines of the UK/US ‘name and shame’ approach. Markets which have not done this have not developed strong AML processes on the ground – this is a reality.
- Boards and senior management must focus on their role in driving the awareness program. Good leaders focus on key messages and key intermediaries to disseminate these messages in the correct manner. This could be using people; technology; internal media etc. and the messages must be crisp and clear. They must also demonstrate firmness and consistency in their actions - ultimately actions speak louder than words.

7. Independent Testing

Observation

With some exceptions, the internal audit teams in Asia (generally) that check the overall health of the AML program, do not focus enough on higher-risk accounts owing to lack of focus from senior management, lack of system flagging of higher-risk accounts, and a lack of the skill-set needed.

Need

Internal audit teams play a critical role in assessing the overall health of the AML program including specifically the role of the compliance officer, adequacy of AML linked reports for scrutiny, the quality of the STR file and an independent check on higher-risk accounts.

This role of internal audit is diluted in many organisations by a lack of independence from compliance, lack of flagging of higher-risk accounts linked to absence of technology to enable KYC Check/trend monitoring and a lack of focus on higher-risk businesses.

Furthermore, internal audit teams are themselves relatively untrained and do not possess the requisite skill-set needed for a meaningful independent assessment of the overall AML program. AML is increasingly a knowledge-led discipline which needs reviews done by staff with a good intuition on AML issues – this is founded on significant experience, training and ongoing awareness at a high level.

Future Action

- Bank's Senior Management need to review audit reports to see if there is any focus on independent checking of higher-risk accounts and also consider the back-end technology requirements to help identify such accounts even if it is an internally developed rule-based monitoring package to start off.
- Banks must ensure independence of internal audit from the compliance departments to allow internal audit to comment on the quality and timeliness of AML guidance from the AML Compliance Officer and other quality issues linked to the filing process.
- Banks must focus on developing the AML skill set of internal audit staff through training and awareness initiatives. Ideally, key persons within the internal audit structure should have had significant experience on AML issues to allow them to provide the leadership required.

8. Terrorist Financing

Observation

Rohan Gunaratna, Head, International Centre for Political Violence and Terrorism Research, in *Global Terrorism Outlook for 2005*, an IDSS December 2004 commentary says:

“During the past three years, nearly 100 medium-to-large scale terrorist attacks against US, European and Australian targets were prevented. In 2005, Western infrastructure and population centres at home and abroad will remain the primary target of Al Qaeda, its associated and affiliated groups. High profile, symbolic or strategic economic and commercial centres, particularly hotels, banks and energy infrastructure will be susceptible to attack. The bulk of the attacks will be in the global south – Middle East, Asia, and Africa – and occasionally on western soil.

As law enforcement, security and intelligence agencies have invested significantly in detecting attacks, it has become more difficult for terrorists to organize and mount large scale coordinated simultaneous attacks of the scale of 9/11. The world in 2005 is more likely to witness attacks of the scale of Madrid, Bali, Casablanca, Riyadh, Istanbul, Karachi, Beslan, and Jeddah. Until now the attacks in Iraq and Saudi Arabia have been mostly against Western targets. In 2005, Islamist groups are likely to attack domestic regime targets as well.

Despite intermittent operational success against terrorist cells planning, preparing and executing attacks, the worldwide threat of terrorism has not diminished... Training a new breed of conflict management practitioners to draw in and sustain a dialogue between the politically marginalized groups and the government elite is more likely to reduce the threat in the long term.”

Industry is divided on whether terrorist financing remains charities based/other legitimate businesses or whether money laundering techniques using the proceeds of crime, are also now equally important. Some experts believe that the AML focus on charities/ other legitimate businesses is so much that terrorist financiers are now increasingly turning to the crime route to make and move money i.e. money laundering. Our observation is that many countries still do not have good control on charities and hence these are probably still being used to finance terrorism.

However, terrorism financiers have evolved other techniques and cash-intensive front businesses are being brought out to launder the proceeds of drug trafficking and criminal monies. Some are even buying out Money Services Businesses to move their proceeds of crime in addition to using Hawalas (unregistered Money Services Businesses (MSBs)). While Private Bankers have for long thought themselves to be free of terrorist financing risks, recent high-profile cases in South Asia have underscored the importance of state

PwC-IDSS Thought Leadership Series

sponsors of terrorism i.e. a nexus may be emerging in some states between PEPs, corruption monies and terrorist financing.

Interestingly there is a dominant view that banks can perform risk-based due diligence at account opening, names matching and also trend monitoring in the life of the account to catch a suspicious terrorist financing transaction. However, key specialists do not support the fact that banks can go beyond the first two stages. Moreover, terrorists prefer to move money mostly below bank monitoring/reporting thresholds making it all the more difficult to monitor.

Amounts Involved in Terrorist Attacks¹

Terrorist attacks	Date	Operational cost (est.) USD
Bishopsgate Church Bombing (UK)	April-1993	\$5,500
African Embassy bombings (Tanzania and Kenya)	August- 1998	> \$30,000
USS Cole bombing (Yemen)	October -2000	\$5,000 - \$10,000
World Trade Center/Pentagon (USA)	September- 2001	> \$500,000
Djerba Mosque bombing (Tunisia)	April - 2002	\$20,000
Attack on Limburg (Yemen)	October - 2002	\$127,000
Bali Bombing (Indonesia)	October- 2002	\$74,000

The associated transactions are usually not complex. The 9/11 Commission 2004 report states that the Al Qaeda funded the hijackers in the US by three primary and unexceptional means: (1) wire transfers from overseas to the US, (2) the physical transport of cash or traveller's checks into the US, and (3) the accessing of funds held in foreign FIs by debit or credit cards. Once in the US, all of the hijackers used the US banking system to store their funds and facilitate their transactions. More generally terrorists are most likely to disguise transactions as study grants, grants for medical treatment abroad, and maintenance allowance from family to keep it outside the purview of scrutiny of FIs.

We do agree with the observation that at the final 'integration' stage of terrorist financing, the monies required for the final terrorist act are so small that it is virtually impossible to detect any 'trends'. At best a names matching can be done. However, terrorist groups do require money at different levels of necessity, most important of which is to survive. They require 'operational funds' to finance local cells and to carry out terrorist operations. The

¹ Modified from "Terrorism Financing: Roots and Trends of Saudi Terrorism Financing," report prepared for the President of the UN Security Council by Jean-Charles Brisard, 19 December 2002

PwC-IDSS Thought Leadership Series

groups also require ‘organizational funds’ to maintain networks of support, communications, training facilities etc and most importantly to underwrite the costs of local conflicts as Al Qaeda is known to be doing in the Middle East, the Caucasus, South and Southeast Asia and in the Horn of Africa. Operational funding constitutes only about 10 percent of the group’s financial requirements.

Terrorist Groups Financial Needs²
<p style="text-align: center;"><i>Infrastructure</i> Communication, Networks, Training Facilities, Protection (90%)</p>
<p style="text-align: center;"><i>Operational</i> Day to day money, terrorist attacks planning & execution (< 10%)</p>

Hence in the placement or layering stages of terrorist financing, where charities or front businesses are used, banks have a clear opportunity to identify suspicious activity although they may not be able to state that it is terrorist financing. For STR filing purposes the standard is just ‘reasonable cause to suspect’.

However, for the smaller transactions, even if just a name matching is done properly, having AML controls in place in FIs would help security and intelligence agencies track down the perpetrators of future terrorist acts. For instance, with the help the money trail revealed during the trial of four terrorists convicted for their role in the 1998 terrorist bombings of the US embassies in Tanzania and Kenya, the US Customs Service’s Operation Green Quest could unravel the financial and support network in several countries. Controls in the banking system can help identify parties after a terrorist attack as well as serve as an alert system that may even help prevent an attack by allowing investigators to identify a new plot before it is executed. Cases exist where a suspicious transaction report filed in a particular city helped uncover a plot for an attack in another city or another country.

The overwhelming opinion of banks is that terrorist financing STRs add value to set-off an investigation and during an existing investigation i.e. with some exceptions, the broad consensus is that banks can play an important role in fighting terrorist financing.

Banks want enforcement to share more names on terrorists with them although they are divided on whether this should be done through the route of published lists or through secured channels. Our personal view is that given the sensitivity of information, secured

² Modified from “Terrorism Financing: Roots and Trends of Saudi Terrorism Financing,” report prepared for the President of the UN Security Council by Jean-Charles Brisard, 19 December 2002

channels are preferred as law enforcement is normally cautious about sharing information that could compromise an investigation.

Need

It must be understood that while the amounts required for the final act of terrorism is small the total amounts needed to recruit, train and sustain terrorists is huge. Charities, cash-intensive businesses, MSBs and Hawala's will continue to be favourites for terrorist financing.

Banks and FIUs need to work together to fight terrorist financing.

Future Action

- Many countries in Asia need to tighten control on charities – not just on paper but actual effective control. This may involve central registration requirements for all charities and controls on the cross-border movement of monies – one bank/branch for all foreign contributions. Countries like India have used these systems for years to combat domestic terrorism.
- Many banks have started avoiding MSBs altogether although this will not work for the system as a whole. Supervisors need to clamp down on MSBs in terms of AML inspections for monitoring effectiveness of their AML rules. This is especially true for Asia. Furthermore, supervisors should issue guidance to banks on providing banking services to MSBs on the lines on the US FinCEN/other agencies guidance of April 2005 (along with the additional FinCEN guidance issued to MSBs) and the Wolfsberg principles on Correspondent banking covering the review of ownership, control, business, and AML policies. Regulated status may not be sufficient; many MSBs have a long way to catch up with banks in AML practices. The safer option in many countries may be to review their actual AML practices.
- Banks in Asia should also be careful of businesses masquerading as something else but actually Hawalas (from an AML & CFT perspective). The FinCEN 6th SAR Review highlights some red flags to watch for.
- FIUs in Asia should work with banks to distribute more names of terrorists through secured channels, such as through identified bank staff and agreed upon procedures.

9. STR Filing

Observation

On defensive reporting (the practice of filing STRs to cover the bank's risks wherever the bank is not sure, without adequate effort to establish 'reasonable cause to suspect') the dominant viewpoint appears to be that this is happening. A minority view is that this is a major problem that stems from regulatory action and will depend on the regulatory/ law enforcement oversight and attitude.

Our personal opinion differs slightly from both the above views. Defensive reporting is certainly a fact of life in the UK/US and also for UK/US banks operating in Asia. However, the broader approach to STR filing in Asia is a very conservative one and in practice there seems to be an implicitly higher threshold for reporting. In some smaller banks they actually implicitly look for 'knowledge' rather than 'reasonable cause to suspect' and this causes significant delays in filing. We believe that overall STR filing is underreported in Asia. For many smaller banks, STR files are empty. Smaller banking branches in Asia appear concerned about possible customer service implications of filing STRs and also their own legal position should the STR be used in evidence in court. In many countries STRs are not admissible as evidence or if admitted the bank is shielded from possible suits through legal provisions.

Law enforcers and regulators in the US and the UK complain of low quality STRs – both inadequate and inaccurate information. STRs are invaluable in an investigation. The Hong Kong police highlighted in 2004 “The problem is that criminals know that banks and law enforcement are nation based. Criminals know that now cost effectiveness in investigation is important and they see an opportunity to use these weakness at the key to a massive organized multi-jurisdictional fraud as was uncovered in a Operation ‘Roystar’ (syndicated boiler room fraud). The case highlighted the importance of STRs both before and after arrest action”.

While STRs rarely trigger off an investigation by themselves, law enforcement anti-financial crime investigators in the UK state that they are of great value during an investigation. Investigators look at all the links of a criminal to other persons and cash-intensive businesses. They also look through the national FIUs database of STRs and in many cases they get hits with old STRs going back 3-4 years. In any investigation, the criminal's personal relationships are a key aspect to map out as they prefer to use persons who do not have any criminal records to front their operations. Investigators try to map out all links and loops so that the entire criminal network can be uncovered - STRs play a key role in this.

Need

There is a need for a 'back-to-basics' approach with smaller banks in Asia on STR filing issues – the reporting standard, the implications and quality issues.

Future Action

- The FIUs need to drive the ‘back-to-basics’ awareness campaign especially amongst the smaller banks in order to clarify key STR filing issues while keeping a focus on quality of STR filing rather than the quantity. Training seminars and presentations to banks and monitoring of filed STRs for quality, will lead to this.
- The US FinCEN (the FIU) released in November 2003 a guidance package designed to assist FIs in the preparation of Suspicious Activity Report (SAR) forms and to improve the quality of information provided in SAR narratives. Asian FIUs could issue similar guidance to their reporting institutions.

10. Feedback from FIUs

Observation

There is an overwhelming agreement amongst banks that more feedback from FIUs in Asia (generally) is needed to make the system more transparent and also to help them to improve their AML efforts.

There is also an overwhelming agreement amongst banks that the reason that feedback from FIUs in Asia (generally) is lacking is because FIUs have resource constraints (money, staff, technology, and training) which governments need to act on. Our opinion is that it is not all about resource constraints and that many FIUs simply do not appreciate the importance of feedback.

While a few banks believe that feedback is needed on each STR filed, most would be happy with periodic (monthly/quarterly) STR analysis reports sector-wise i.e. US FinCEN SAR Review style. We believe that where an investigation is completed and the FIU has not found anything a ‘closed our files’ letter to the bank is a key factor for the banks comfort with the customer. In some countries, FIUs do this.

There is an overwhelming agreement amongst banks that feedback from FIUs in comparison to peers is meaningful if peer groups are relevant and is used as a basis for further investigation, rather than drawing conclusions on the quality of the AML program.

Need

More feedback is needed from FIUs in Asia of the standard/ quality of the US FinCEN SAR Review. Such feedback should be circulated more broadly to the accounting/ legal community also in addition to just FIs.

There is need for benchmarking of STR filing vis-à-vis peer groups as a starting point for a more detailed review of AML Program quality.

Future Action

- In line with the revised FATF 40 Principles, FIUs in Asia should commit themselves to providing more feedback to reporting institutions on the lines of the US FinCEN SAR Review.
- FIUs should make relevant peer groups of their reporting institutions and draw comparisons of STR filing both in the country and perhaps benchmarked with practices in the US, UK through liaison with their counterparts in these countries.
- We are also in favour of close-door feedback to reporting institutions where the quality of STR filing is poor or their filing patterns are way out of line with their peers indicating possible AML program shortfalls. In such an eventuality, the supervisor should also be tipped off so that AML inspections focus on program quality issues.

PwC-IDSS Thought Leadership Series

- Governments in Asia (generally) need to address the resource constraints of FIUs so that they are in a better position to fully address the need for reverse feedback to reporting institutions.
- Many FIUs in Asia need to develop a better working relationship with the FIs filing STRs with them. This will also help to emphasise the importance of feedback from the point of view of the reporting institutions.

11. Guidance from Supervisors

Observation

Banks appear divided on whether more prescriptive guidance is needed (with the risk that banks take on an unthinking “tick-box” approach) or broadly descriptive guidance (with industry bodies giving more prescriptive guidance) so that banks have adequate flexibility. Our opinion is that prescriptive guidance is needed as without this, substandard implementation in the smaller banks is almost assured as they rely on the force of law to motivate them for action. However, a good public consultation process is also needed with industry groups/ key banks providing feedback through this process.

Need

AML guidance from supervisors in Asia has tended to be descriptive laying out the overall framework/ principles alone. This needs to change as the standards of on-ground implementation differ widely amongst the larger banks vis-à-vis the smaller banks and amongst US/UK banks vis-à-vis local banks.

Future Action

- More prescriptive guidance (focussed on risk and quality issues) based on a well-executed public consultation process in which industry groups are ‘actively engaged’.

12. Technology

Observation

Steve Farrer, Director, Business Development for AML and Fraud Detection Solutions, ACI Worldwide (Asia) says “Without sophisticated AML technology large banks simply don’t have a fighting chance to detect money laundering effectively. Inevitably, they will ultimately spend more in penalties, legal costs and finally purchasing the technology, than if they had been proactive upfront”. *Jim Wills*, Business Line Manager for AML, Searchspace UK says “Our general perception in Asia, is that unless AML becomes a key issue at the country level, then the institutions will not invest in AML technology”.

Traditionally, supervisors have shied away from getting involved with technology issues many denying that this is their role at all. However, AML is increasingly becoming a technology driven discipline and needs active involvement of supervisors to set standards and create market size so that technology solutions become more affordable for smaller banks. There is a broad consensus amongst banks that supervisors should become more actively involved in AML technology issues. We agree with this view fully.

There is a dominant view amongst banks that technology (trend monitoring software (for AML), names analysis software and linked KYC data-bases) is essential for AML/CFT monitoring purposes and a regulatory rule is required like that adopted by the Swiss Supervisor. In Switzerland, all financial firms must have the necessary transaction monitoring systems and technology to facilitate detection of suspicious transactions. However, firms below a certain size will not have to install software and instead will have to undergo annual external ‘know your customer’ and continuing due diligence audits. Swiss banks have three alternatives for action: they can either build their own software products, they can group together to build a common system; or buy a commercial package.

Our opinion on the build-or-buy decision is that with rare exceptions, building a sophisticated technology (for example, neural networks, statistical and profiling engines) in-house is clearly out of the ‘core competence’ of most banks. There are good external vendors from amongst whom banks can pick and choose a package that most adequately meets their needs. Setting up the technology package is a critical task to ensure that the ‘false positives’ (redundant alerts) are minimised – data consolidation and quality issues will need to be addressed. Even if a state of the art technology package is purchased, bad inputs will lead to bad outputs – this fundamental equation will not go away. Without flagging of higher-risk businesses and basic business data, meaningful peers groups cannot be created. Transaction trend monitoring software compares a transaction with the history on the account and with its peers; a transaction may be suspicious when reviewed at the customer level even if not at the account level – this sort of sophistication is difficult to build into a “home grown” package that would probably be little better than a basic rules based system.

PwC-IDSS Thought Leadership Series

Technology pricing is another issue. Most vendors have got used to pricing by US/UK standards which when translated to local currencies in Asia are prohibitively expensive. Vendors do not think they are overpriced (naturally) but local banks in Asia cringe on hearing their quotes. The US/UK banks in Asia are more open to the price quotes as their technology adoption is driven out of head office requirements.

Need

Many banks do not have adequate in-house technology assessment processes in place and are also not ready to commit resources to get outside assistance. The proliferation of vendors as a result of the USA PATRIOT Act has also led to a lot of confusion on who are quality vendors, and what is an acceptable standard.

While technology is part of a package of AML strategies, adoption of technology for AML/CFT purposes is increasingly essential and supervisors should accept this fact.

Technology prices need to be cut in Asia by 30% or more – this can only happen through the demand and supply equation – if market demand is substantial, vendors can be ‘persuaded’ to cut prices.

Future Action

- Supervisors should take the cue from the US FDIC Nov 2004 broad technology due diligence standards to craft something similar for their regulated entities. They can also ask industry bodies to work on more detailed guidance.
- Supervisors can set broad accrediting standards and a process (however implemented) for vendors so that banks know who is up to standard.
- Supervisors should introduce a regulatory rule requiring AML technology on the lines of the Swiss rule.
- Supervisors can also work in groups (e.g. ASEAN) with key vendors to create market size and ensure that vendors cut prices.

13. Personal Accountability and Professionalism

Observation

One respondent stated candidly “senior management must be held responsible for the risk. After all, they tend to benefit disproportionately, in the rewards.”

There is a general need to increase the focus on personal accountability of senior management in Asia to drive AML practices. While most banks prefer more prescriptive guidance as the solution, without a degree of ‘name and shame’ focussing on management and the banks themselves, we suspect personal accountability cannot be underscored by supervisors. At the minimum, where considered appropriate, confidential but forceful letters of reprimand from supervisors are necessary.

On professionalism, there is a broad consensus that a UK style annual report on AML issues along with professional accreditation (AML qualifications) is essential. The issue of whether there is any association that offers a suitable standard of AML qualification is not the one that has an easy answer as there are many players in this space. Some respondents also stressed the importance of industry bodies being active and the MLRO to be a senior experienced person with a senior reporting line.

Need

AML budgets for technology/ consulting services are sadly lacking in most banks in Asia. Key to driving spending on AML to the required levels is focus on personal accountability of senior management – this will loosen purse strings. Personal accountability may be enshrined under the broader banking regulations act but without the supervisory AML rules emphasising this aspect separately, action from senior management will not be forthcoming.

UK style MLROs annual report to management/ the supervisor along with suitable professional accreditation is a must going forward.

Future Action

- Supervisors in Asia need to put their words into action through regulatory actions and fines – focusing on both management and the bank. More prescriptive AML rules focussing on personal accountability are also needed.
- The UK Joint Money Laundering Steering Group (JMLSG; under the British Bankers Association) guidance notes format for the MLROs Annual Report should be adopted by Supervisors in Asia.
- Professional accreditation is a key means to ensure that the AML Compliance Officer is suitably trained. There is currently no world standard body that suitably advocates an AML best practice training that is of sufficient coverage and depth. One approach can be for industry bodies to engage existing professional bodies to review and enhance their training material with the help of consultants.

14. Public Awareness

Observation

There is a general consensus that public awareness – of customers and of staff as members of the public – is important/ critical to have so that it reduces customer resistance to KYC practices. Our opinion is that public awareness is critical and is a much ignored area. Initiatives to build public awareness will also lead to higher levels of top-of-mind recall of staff especially for smaller banks and the non-banking institutions sector.

In the UK, the FSA has started a KYC awareness campaign that is designed to raise awareness among the general public about the important part they can play in combating financial crime. It hopes to reduce ‘resistance’ to identification checks and the resulting problems that firms are experiencing when prospective customers walk out or complain. The campaign materials are simple posters (for staff awareness) and leaflets (for customer awareness) carrying the endorsement of the authorities. These are available for FIs to use when communicating with their customers, for example in customer mailings, posted in branches or offices, or in information packs. The campaign is intended to be a long-term one rather than a quick, high-impact campaign. The materials are of most relevance for private retail customers, although firms can use them for other customers as well. The messages are also relevant to staff.

There is a broad consensus that building public awareness is the responsibility of all key players in the AML space – big banks through their public relations campaigns, industry bodies, supervisors and the FIUs.

Need

Public awareness on KYC issues/ the fight against financial crime is critical to build up and all key players need to get involved.

Future Action

- All key players in the AML space need to focus on the issue of public awareness
- Supervisors and industry bodies in Asia can adopt the UK FSA style ‘posters and leaflets’ campaign
- FIUs can set up an incentive based Hawala reporting hot-line

Acknowledgements

We have received completed questionnaires from the following respondents who responded in their personal capacity. We have quoted them in our paper wherever agreed by with the respondent. One respondent has chosen to be anonymous.

- Madam Koid Swee Lian, Director of the FIU, Bank Negara Malaysia
- Elizabeth Cheang, VP Compliance and Fraud Investigations, HSBC Singapore and Chairman of the Association of Banks (ABS) Financial Crime Task Force
- Peter Hazlewood, VP International AML Compliance, JPMorgan Chase Banking Corporation, USA
- Steve Farrer, Director, Business Development - AML and Fraud Detection Solutions, ACI Worldwide (Asia) Pte Ltd
- Chris Wilson, Director AML APAC, UBS AG, Hong Kong
- Jim Wills, Business Line Manager for AML, Searchspace, UK
- Srinivas Vishnubhatla, Vice President Business Development, IntegraScreen (America) Inc, USA
- Martin Chung, Regional Head of Money Laundering Detection, Asia, ABN AMRO Bank, Singapore
- Jos de Wit, former Group Compliance Officer, ING Group, Netherlands
- Jay Jhaveri, Director Asia World-Check, Singapore