The Changing Regulatory Landscape

7–8 October 2015
Kuala Lumpur
Malaysia
Rapporteurs

Accounting Research Institute,
Universiti Teknologi MARA (UiTM),
Shah Alam, Malaysia

• Professor Dr Rohana Othman
• Professor Dr Zaiton Hamin
• Saslina Binti Kamaruddin
• Siti Saidah Nafisah Binti Omar
• Mohd Muaz Abdul Hakim
• Hayyum Suleikha Selamat
• Zulaikha Amirah Binti Johari
• Salwa Binti Zolkafil
The evolution and ever-changing nature of the financial landscape has unveiled new and emerging threats, including trade-based money laundering, the terrorist threat of ISIS and cyber fraud to mention a few. These developments have led to numerous regulatory reforms globally and, in particular, in relation to Financial Crime and Terrorism Financing. As a result of greater expectations from the regulators, it is imperative for financial institutions to be able to respond swiftly and effectively to new developments and the changing "rules of the game", as well as being supported by effective supervision. The cumulative effects of these trends is forcing the financial industry to fundamentally reassess business models and operating practices.

The 7th International Conference on Financial Crime and Terrorism Financing, themed “The Changing Regulatory Landscape”, aimed to shed light on the recent overhaul of the regulatory framework and discuss the balance between comprehensive and intrusive means to strengthen regulations, as well as to look at ways of increasing the resilience of financial institutions to better combat the threat of financial crimes and terrorism financing.
Welcome Address

Kwan Keen Yew
Group Chief Compliance Officer, CIMB Group

The Conference commenced with the welcome address from Mr Kwan Keen Yew (Group Chief Compliance Officer, CIMB Group). Mr Kwan reminded delegates that new threats had appeared on the financial landscape, including trade-based money laundering, the funding of new terrorist threats and cyber fraud. Such developments have led to the creation of numerous regulatory forms globally and, in particular, relating to financial crimes and terrorist financing. He emphasised that this year’s Conference theme was a result of a greater expectation from regulators for financial institutions to be able to respond swiftly and effectively to new developments and trends.

Mr Kwan briefly explained that the Conference was designed to include plenary and concurrent sessions to provide for broader understanding of the strategies to be adopted in designing globally-effective compliance programmes. He emphasised that the expert line-up of Conference speakers and panellists included senior representatives from both domestic and international agencies who were experts in their respective areas. Other speakers included representatives from major financial organisations and industry suppliers who could share both insights and best practice in their respective fields. He had high hopes that the delegates would be able to incorporate and apply learnings and insights from the Conference for the benefit of their own organisations.

Mr Kwan continued his speech by noting that Malaysia is committed to global efforts and best practice to tackle financial crimes and terrorist financing. He further elaborated that the success of such efforts would depend on on-going dialogue and collaboration as well as the sharing of knowledge between key stakeholders at national, regional and global levels. On behalf of the organisers, he hoped that IFCTF 2015 would play a key role in facilitating such discussions and collaboration. He also expressed his gratitude for the participation of so many professionals and experts.

Mr Kwan thanked the core organising committee whose members had worked hard to make the Conference possible. He also applauded the sponsors such as LexisNexis Risk Solutions, BAE Systems, Dow Jones, Swift, TESS and Thomson Reuters. He concluded his welcome address by thanking the audience for their attention and wished them an enjoyable Conference.

“Malaysia is committed to global efforts and best practice to tackle financial crimes and terrorist financing.”
The keynote address was delivered by YBhg Datuk Haji Mustafar bin Haji Ali, Deputy Chief Commissioner (Prevention) of the Malaysian Anti-Corruption Commission (MACC).

Datuk Mustafar then pointed out that Malaysia has just completed the Anti-Money Laundering and Counter-Financing of Terrorism (AML/CFT) mutual evaluation exercise. He was pleased to note that the Financial Action Task Force ( FATF) had recognised the robustness of Malaysia’s national AML/CFT policy framework and the country’s seriousness in fighting financial crimes. He also noted that domestic AML/CFT co-operation was effective and well developed at both the strategic and operational levels. The National Coordination Committee (NCC) played a significant role as the centre for the co-ordination and co-operation of Malaysia’s strategies and in implementing a shared culture of AML/CFT compliance amongst the public and private sectors. The mutual evaluation report 2015 highlighted that the inter-agency co-ordination amongst policy makers, regulatory authorities, supervisory units, the financial intelligence unit, and the special task force had achieved significant outcomes within Malaysia’s AML/ CFT regime.

Datuk Mustafar observed that the evaluation report also emphasised the need to address some gaps in the area of terrorism financing. The overall compliance level indicated a strong legal and regulatory framework for preventive measures which signified Malaysia’s commitment to fighting such financial crimes. Consequently, he believed that such a positive evaluation would strengthen foreign confidence in the Malaysian financial system and the country’s economic development. He contended that it was then the responsibility of the financial institutions together with the public and private stakeholders to continuously assess and undertake the necessary improvements to inter-agency collaboration aimed at eradicating financial crime.

He noted that any negative perception by international stakeholders of the Malaysian AML/CFT measures might significantly upset the economic wellbeing of the country and international co-operation between Malaysia and her foreign counterparts.

Datuk Mustafar indicated that strong collaboration between the financial institutions and law enforcement agencies was imperative for effective enforcement efforts in addressing financial crimes. To illustrate the importance of this inter-agency collaboration he shared a successful collaborative initiative between Bank Negara and the Royal Malaysian Police, as well as the financial institutions, known as the Mule Account Holders, in preventing the abuse of the financial system. He explained that under this initiative Bank Negara together with the Royal Malaysian Police shared information about individuals identified as being under the Mule Account Holders Initiative to financial institutions in order to enable them to manage the risk arising from these mule accounts and to avoid enabling fraudulent transactions. This collaborative initiative saw a 23 percent increase in the submission of Suspicious Transaction Report (STR) by financial institutions over a two-year period from a marginal 4 STRs in 2012 to 97 STRs in 2014. The major increase in the disclosure of STRs on Mule Accounts was due to the Royal Malaysian Police.

Datuk Mustafar further observed that in 2013 the NCC had endorsed and adopted the Malaysian National Risk Assessment on Money Laundering and Terrorism Financing. This assessment indicated five types of crimes that were creating high money laundering risks or threats to Malaysia, namely fraud, drug trafficking, corruption and bribery, smuggling offences and tax crimes.
Datuk Mustafar believed that corruption and bribery are very likely to become trans-national or cross-border crimes. He supported this view by referring to Transparency International, which highlighted the fact that currently cross-border bribery was an emerging risk in the ASEAN region. Nevertheless, he said given the different legal and regulatory expectations, the implementation of effective international or regional efforts to combat such crime could be challenging. For instance, while all Southeast Asian countries took a serious view of bribery, differences in the definition of bribes cause hurdles in trans-boundary co-operation.
An example he gave was the ‘facilitation payment’ which was exempted from criminal prosecution in some countries. He argued that such differences could lead to political concerns or lack of legal cooperation across borders. As such, he warned that this was probably an area that financial institutions with regional operations should pay close attention to and consider establishing appropriate mitigating measures.

Datuk Mustafar then focused his attention on financial crimes within the ASEAN region. He noted that 2015 marked a significant milestone for ASEAN as the ASEAN Declaration on the economic blueprint will bring about the implementation of the ASEAN Economic Community by the end of 2015. Following this implementation, he said that of interest to the financial sector would be financial services liberation, including banking integration. He observed that with the ultimate aim of achieving financial services integration, some financial services have expanded their activities across the ASEAN region. For instance, some Malaysian banks have a presence in Indonesia, Thailand and the Philippines, as well as some other countries outside ASEAN. He warned that while the benefits of cross-border operations are recognised, the accompanying risks, if left unchecked, might pose a threat to the integrity of the financial system. He said that such cross-border financial operations might be abused as a means to facilitate financial crime. He highlighted that, as the ASEAN community marked its regional milestone, financial criminals have also become more sophisticated than ever before. Because of such criminal enterprise, public and private financial bodies must move away from their conventional ways of operating domestically and co-operate regionally.

Datuk Mustafar then alluded to the problem of cross-border deterrence and detection of financial crimes. He stated that different regional regulators have different expectations. Given such differences, those financial institutions that have operations abroad need to be able to respond adequately and swiftly to the threat of cross-border financial crimes. Any lack of swift response could ultimately impact the integrity of the financial system domestically and internationally. In line with the theme of the Conference, he believed that it was only appropriate that this critical regional regulatory expectation, as well as ways of cooperating, were discussed to preserve the integrity of the financial system. The regulators have significant expectations on the roles and contributions of the financial institutions in supporting the national agenda to combat and reduce financial crimes, including terrorist financing. He highlighted a recent report by an international integrity body, which quoted corruption as the top issue across ASEAN countries.

Datuk Mustafar then shared the MACC initiative in dealing with corruption in Malaysia. He explained that in 2011 the MACC introduced the Corporate Integrity Pledge (CIP), which was a unilateral declaration by a company to show its commitment not to commit corrupt acts and to work together with the MACC towards creating a business environment that was free from corruption. Datuk Mustafar was pleased to mention that nearly 600 institutions and corporations have committed themselves to the CIP since its inception. However, he noted that a negligible percentage of these pledges were from the financial sector. He emphasised that despite the fact that the CIP was not a regulatory or mandatory instrument, signing the pledge was imperative as it would signify a company’s commitment to fighting financial crimes. He also said that such a commitment would be in line with the national anti-corruption principles for corporations in Malaysia. The CIP was consistent with the model adopted in the ten principles of the United Nation Global Compact 2000. He then took the opportunity to urge the financial institutions and other organisations present to commit to this pledge.

As a concluding remark, Datuk Mustafar reiterated the importance of extensive cooperation and collaboration among the regulators, the financial industry and the law enforcement agencies both domestically and internationally, which would assist in protecting the integrity of the financial system against criminal abuses. In ending his speech, Datuk Mustafar quoted Abraham Lincoln’s annual message to Congress in 1862: “The dogmas of the quiet past are inadequate to the stormy present. The occasion is piled high with difficulty, and we must rise to the occasion. As our case is new, so we must think anew, and act anew. We must disenthrall ourselves and then we shall save our country.” Datuk Mustafar stated that there was a need to think anew and act anew to fight corruption, money laundering and other financial crimes. He further said that there was a need for change and such crimes should be seen from a new perspective. Such a new approach would inevitably be imperative in dealing with financial crimes in the future. On that note, Datuk wished all the delegates productive and fruitful discussions during the Conference and hoped that they would benefit from the exchange of views on key AML/CFT issues.
Changing Regulatory Landscape - A Regional Perspective

Mohd Zabidi Md Nor, Director, Prudential Financial Policy Department, Bank Negara Malaysia

The local financial sector could learn from the world’s largest banks abroad by adopting a proactive approach to compliance and making crucial forward-looking investments.

Mohd Zabidi Md Nor

Decisions made by the compliance officer could then even be ignored. He elaborated further that the greatest implication of such negative perceptions is the difficulty in attracting and retaining talent in the compliance function because everyone wants to be part of a successful team and does not wish to be associated with a negative image. He reiterated that, although a compliance team was imperative in any financial institution, everybody else in the organisation was taking them for granted.

He then explained that the reasons and catalysts to the paradigm change after the GFC involved three fundamental elements. First, the unprecedented penalties and fines for non-compliance that were attributed to legislation such as tax evasion laws and the Anti-Money Laundering regime. Mr Zabidi stressed that the impact of such fines and penalties affected the reputation of financial institutions. He warned that the moment any financial institution appears in the headlines in this way, its hard work over the years crumbles and its reputation is tarnished. The second factor was the fact that the regulatory environment became more complicated than previously. He pointed out that the emergence of new types of technology and terminologies were a challenge to compliance officers even though it was useful to the business team.

The third catalyst was a regulatory structure which focused more on the institutional structure and compliance enforcement. He added that the Banking and Financial Institutions Act (BAFIA) 1989 had been replaced by the Financial Services Act 2013 and it was entirely different regarding the spectrum of enforcement mechanisms. Previously, non-compliance issues had had many constraints because, under the BAFIA 1989, everything would be seen from the perspective of the criminals. However, under the Financial Services Act 2013 the complete spectrum of enforcement mechanisms covered everything from criminal to administrative sanctions.

Mr Zabidi then suggested the way to achieve a more sustainable paradigm: that any change should be driven by need rather than by fear. Furthermore, this new paradigm would comprise of three components: meeting expectations (ensuring conformity to relevant requirements); maximising efficiency (eliminating redundancies and costs); and adding value (enhancing the business by providing a competitive edge). He then suggested that by using standard setting, the local supervisory authorities
The Changing Regulatory Landscape

Mohd Zabidi Md Nor

Ida Rumondang

Mad Yusof Yazid

would facilitate the development of a strong compliance culture through minimum standards and industry engagement. Closer to home, he then explained the Bank Negara Compliance framework which provides a new standard for Malaysian financial institutions. The standard focuses on oversight arrangements and the establishment of an empowered and competent compliance function.

Moving beyond the minimum standards, Mr Zabidi indicated that optimising compliance costs and exploring the potential for enhancing the business should be the way forward. He contended that compliance had been the main component in the effort to rebuild trust in finance. He concluded his presentation by suggesting that the local financial sector could learn from the world’s largest banks abroad by adopting a proactive approach to compliance and making crucial forward-looking investments. He highlighted the three elements of proactive compliance: first, effectiveness (comply with the minimum standards and laws); second, efficiency (comply with the minimum costs and minimise duplications) and third, enhancement (compliance to achieve optimal balance – independent and value-adding to the business).

Ida Rumondang, Deputy Director, Banking Research and Regulation Department, Indonesia’s Financial Services Authority (OJK)

Ms Ida Rumondang began her presentation by highlighting the current regulatory challenges and arbitrage. She explained that such issues and the fight against money laundering were rather daunting, particularly in an enormous country like Indonesia. She argued that it was easier to make a regulation rather than to implement it. She observed that, compared to Malaysia, a key regulatory challenge in Indonesia was the financial exclusion of a large proportion of the population where there was a high rate of non-banking. The national identity cards system did not cover all residents in Indonesia and without an identity card such people could not access any financial institutions. Another regulatory challenge was the increase in cybercrime due to the increasing number of hackers.

She explained further that there were various sizes and differences among the banks in Indonesia. There are some 1600 rural banks and it is not easy to set the standards for them all,
particularly in terms of developing a database of Politically Exposed Person (PEPs) and terrorists. Ms Ida noted that the main challenge was not the size of the bank, or even the size of the data, but the size of the transaction.

On the issue of regulatory arbitrage, she explained that criminals in Indonesia would usually deposit their money in Singapore because they thought that “no evidence of the crime equals no punishment for the crime.” She gave as examples crimes concerning corruption, false accounting, illegal logging, shadow banking, human trafficking and transfer pricing as some of the illegal activities that occur in her country. Another problem is the ability to open global accounts online, which do not require any face to face meeting. She explained however that in Indonesia it is compulsory for banks to meet their customers at least once.

As for regulatory expectations, Ms Ida pointed out that not only was it expected that financial institutions follow all international recommendations and standards, but that they would also have to comply with all relevant national laws and regulations. Besides, they should also have an effective AML compliance framework in place. In terms of international standards, she cited the FATF 40 Recommendations, United Nations SR1267 and SR1373, FATF Mutual Evaluation Reports and Basle AML index as being significant. The banks in Indonesia she noted were regulated through the relevant AML laws and regulations for fund transfer, the law and regulations on the Prevention of AML 2010, the law and regulations on Eradication of Terrorism Financing 2013 and Bank Indonesia guidelines on AML and terrorism financing. She noted that most of the Indonesian banks mistakenly believed that financial crime such as terrorism financing would involve a considerable amount of money. However, she pointed out that a terrorist only needs USD$20 to make a bomb.

Ms Ida emphasised that information and communication technology (ICT) has become more sophisticated than before, enabling the spread of information and the recruitment of potential bombers through the Internet. She then shared her experience on how she detected a terrorist who was requesting donations through a website. She explained that in Indonesia the Ministry of Communication and Information had selected volunteers throughout Indonesia to monitor Internet usage in order to detect illegal and immoral acts such as engaging in pornography or terrorism.

Ms Ida concluded the session by explaining the minimum standards taken by the Indonesian Government on suspicious transactions. She emphasised that having a set of minimum standards that was applicable across the country was better and easier for a bank. However, she also warned that the minimum standards must be carefully developed so they could be implemented across a wide range of banks and countries and thus avoid any negative repercussions.

She also explained that the standard operating procedure (SOP) regarding cooperation among law enforcers in different countries should be agreed for the benefit of policing financial crimes across the region. It was also crucial to establish the minimum information needed for transfers and the requirements to be a correspondent bank. She finally cautioned that in developing the technologies used to provide designated services, banks must incorporate assessing money laundering and terrorist financing risks before adopting such technologies.

Q & A Session

During the question and answer session, the speakers responded to the issues raised by the moderator, Mr Mad Yusof. The first question focused on the reasons for the negative view of compliance officers. Mr Zabidi replied that these negative perceptions belonged in the past. Previously, compliance officers were thought to be just following the instructions from the board rather than thinking about what to achieve. Mr Zabidi was of the opinion that the new generation of compliance officers have changed that perception.

The second question posed to Ms Ida was on how to measure the effectiveness of compliance officers. She responded that the important thing was that compliance officers should know their bank. She suggested that the questions they should ask were about where the high risk was, when the increased risk would occur and who posed the greatest risk. The answers to such questions would dictate the appropriate response to the issues. She argued that having high end technology was not the answer because, in spite of all the precautions that could be taken, problems could still arise and sometimes small but important things could be neglected.

On the final question from the floor about the appropriateness of relying exclusively on compliance officers to comply with the regulations, Mr Zabidi said that it was part of the board’s responsibilities to ensure the balance between business oversight and the role of the compliance officers.
The moderator, Ms Foo Lei Mei, commenced the session by highlighting the current issues of money laundering and terrorism financing as global concerns. She said that the aims of the session were to assist in the understanding of the requirements of compliance in financial institutions to prevent money laundering and terrorism financing. She argued that this was crucial in assisting in understanding the causes and unintended consequences of de-risking. She then referred to the IMF global estimate that around USD2 trillion in illegal proceeds arise every year. Consequently, regulators are demanding that financial institutions must establish a good compliance framework. The FATF also revised its standards and requirements as well as its assessment methodology in 2013. She noted that in implementing a compliance framework costs remained the biggest challenge for financial institutions. To support her argument, she cited the KPMG global survey in 2014 which said that compliance costs for AML in the banking sector alone have increased by 53 percent. Ms Foo observed that institutions globally have begun to assess and review their risk assessments. She then invited the first speaker to give his presentation.

Richard Chalmers, Formerly Co-Chair, Working Group on Evaluation and Implementation, Financial Action Task Force (FATF)

The first speaker, Mr Chalmers, started his presentation by focusing on the FATF standards on risk assessment. He noted that the FATF Report in 2012 and the revision of its standards have centralised the risks of money laundering and terrorist financing. As such, he stated that it was fundamentally important for stakeholders to identify, assess and understand such risks. He added that the role of the FATF was to guide stakeholders on how to understand the risk involved rather than a mechanical process to identify and assess the risk of money laundering and terrorist financing.

He noted that the current FATF standards apply to national policy makers, regulators, law enforcement and regulated institutions. Mr Chalmers urged that there was a need for a revision of the regulatory framework and for there to be an alert on de-risking. He then stressed that the central requirement was to manage the risks involved without jeopardising the company. He advised that financial
institutions should manage the risk and not undertake business that fails to apply the “Know Your Customer” (KYC) rules. Moreover, he pointed out that in managing the risk, it was important to do it appropriately relating both to the system and control. 

Mr Chalmers then went on to explain the need to be concerned with de-risking. He noted the FATF’s view that de-risking involved those using an informal mechanism rather than the conventional banking system. He further observed that such de-risking could reduce financial inclusion objectives as well as the ability to monitor the money trails. Also he stressed that it was crucial to establish guidance papers to reinforce the message on financial inclusion in relation to risk management to the banking institutions and also Non-Profit Organisations (NPOs). He quoted the UK experience of dealing with a high number of unregistered immigrants who required access to financial institutions. He then pointed out that most countries had policies to provide financial services to the migrants in their countries. He noted that the FATF has issued guidance on how to deal with such risks.

Mr Chalmers also explained the impact of de-risking on individuals and organisations. Such individuals or organisations could be money remitters who were transferring money to their countries. He added that organisations that could be affected by de-risking included banking institutions and non-profit organisations. Individuals could also be low-income and undocumented people who could face some challenges in meeting the basic Customer Due Diligence (CDD) requirements.

He then examined the FATF approach to the risks of financial crimes. He paid attention to the recent Malaysian National Risk Assessment (NRA) which, he noted, was due to the engagement of all the stakeholders involved who contributed the much-needed inputs. He said that the obligation to manage risks extended to all the stakeholders including policy-makers, law enforcement, regulators and financial institutions. As a result, the recent APG Mutual Evaluation Report in 2015 showed the success of Malaysia’s efforts to comply with the objectives of the AML/CFT framework.

Mr Chalmers concluded his presentation by suggesting several measures that could be taken to counter risks particularly with the emergence of new technologies. Such counter-measures could be improved by better understanding the risks involved. Also financial institutions should take an active role on how to assess the risk using technology.

Richard Chalmers
the different perspectives of risk and
gave an overview of the issues of de-
risking and re-risking. He examined the
manner in which financial institutions
could end up de-risking and the
associated unintended consequences
of de-risking in the long term. On the
issue of financial compliance Mr Correia
contended that there was a need to
increase the financial penalties for
failure to comply. It was recommended
that banking institutions should
manage their operations according to
a risk based approach. It was pertinent
for banking institutions to conduct
a compliance programme more
vigorously and to increase the number
of compliance officers within their
institutions. Moving on to the issue of
mobile payment providers, he noted
that a compliance programme should
also be implemented to support these
new areas of services.

The use of remittance services
by migrants to transfer money to
their home countries could give rise
to an underground banking system,
known as “hawala”. This is evidently
observed in the Somali case in which
such an informal banking system had
a significant negative impact on the
Somalian economy.

De-risking affects more than just
banking institutions. One of the likely
impacts was a lack of social cohesion
that affects vulnerable segments of
society. From clients’ past experiences,
negative media headlines could be
costly to an institution’s reputation.

In concluding his presentation,
Mr Correia pointed out that more
guidance was needed from the
regulators to highlight the issue of
de-risking, while re-risking needed
a multilateral approach from
different jurisdictions to establish the
appropriate measures in mitigating
those risks.

Q & A Session
During the question and answer
session, the moderator asked the
first question as to whether de-risking
should be a commercial concern
left to the financial institutions
or whether the regulators should
intervene. Mr Chalmers responded
to this question by arguing that,
ultimately, it was up to the financial
institutions to decide on de-risking
issues. He further argued that financial
institutions should take suitable
measures when approaching de-risking.

The second question from the
moderator was on the adequacy of
the FATF standards in dealing with
de-risking issues in the challenging
regulatory landscape. Mr Chalmers
replied to the question by stating
that in principle the standards
were adequate. However, with the
development of new technologies, it
was becoming easier to understand
the customer’s business. Financial
institutions and the regulators should
be concerned about this and form a
common understanding of the risks
involved and how suitable counter-
measures could be developed.

The final question from the
moderator was on the capability of
new technologies to assist compliance
officers to overcome the challenges
of de-risking. Mr Correia responded
to this question by saying that such
technologies could manage their
work more efficiently than before
and compliance officers who might
be constrained by time could benefit
from them. He gave an example from
banking: previously it was difficult for
banks to know the total number of
their customers but now, with new
technology, they were able to
monitor their customers’ accounts
more efficiently.

Mr Chalmers added that in his
experience of supervising in London
he came across a senior management
officer of a financial institution who
could not adapt to new technology
and did not understand de-risking. He
suggested that it was fundamentally
important for the management team to
engage fully with new technologies.
CONCURRENT SESSION 1:

Regional Perspective: Ultimate Beneficial Ownership

Speakers:

Krishna Subramanyan
Director & Head – APAC OneKYC, Citibank

Rezy Izwan Ramly
Director of Compliance, Suruhanjaya Syarikat Malaysia (SSM)

Nicky Antonius

Moderator:

Joseph Ng
Head of Financial Crime Compliance, HSBC

The moderator, Mr Joseph Ng, started the session by highlighting that the topic of “Ultimate Beneficial Ownership”, commonly known as “UBO” was a challenge. He mentioned that the complexity of this topic was related to the exact definition of UBO, the challenge of obtaining the information when it was commonly being protected under the personal data privacy law, and also on the extent to which customers were willing to share their personal information.

Krishna Subramanyan, Director & Head – APAC One KYC, Citibank

Mr Krishna Subramanyan, as the first speaker, began his presentation by focusing on the definition of UBO. He suggested that BO, or the beneficial owner, is any person, including a natural person or entity that can exercise some level of control, directly or indirectly through influence or other means, over an account or the account holder. He then defined direct control of a client entity as a mandate for a person to control the activity of that entity. For instance, it could be through an authorised signatory. In contrast, he explained that indirect control is when a person owns a significant portion or a certain percentage of an organisation, but is not directly responsible for running the organisation on a day to day basis.

He then explained that the UBO of an account is the “natural person” with actual (i.e. explicit) or effective (i.e. implicit) control over the account. Actual control is derived from having explicit authority over the account and its assets (for example, as a trustee). Effective control is derived from an individual’s role in the account or the account holder entity, or from their level of ownership in the account assets or account holder entity that confers such control as follows:

• a role that establishes actual control through a formal mandate of authority (for example, a CEO);
• a role that may carry no formal mandate of authority but confer effective control through authority over a significant portion of the assets of the entity (for example owners of 10% or greater);
• a role that carries no formal mandate of authority over, or entitlement to the assets of an account or account holder entity, but may still permit the exercise of effective control through influence and other indirect means (for example, Chairman of the Board);

The speaker then proceeded to highlight the fact that the FATF Recommendations require countries to ensure that adequate, accurate and timely information on the beneficial ownership of corporate vehicles is available and could be accessed by the competent authorities in timely fashion. He also said that identifying ultimate beneficial ownership has been a difficult task. The standard practice has been for clients to make investments using legal arrangements (i.e. a limited liability company, or offshore company) to shield the name of the “natural persons” who were the ultimate beneficial owners of the investments.

He observed that various agencies and supranational bodies have defined the term “beneficial owner” but, for the most part, they all agreed with the FATF definition, which refers to “the natural person(s) who ultimately owns or controls a customer and the natural person on whose behalf a transaction is being conducted. It also includes those persons who could exercise ultimate effective control over a legal person or arrangement. Nevertheless, he acknowledged that knowing and identifying the natural persons who could exercise ultimate effective control might be a bit more difficult to accomplish and therefore needs to be based on clear internal standards on obtaining such information using “independent resources”.

Rezy Izwan Ramly, Director of Compliance, Suruhanjaya Syarikat Malaysia (SSM)

The second speaker, Mr Rezy Izwan Ramly, began his presentation by asking the audience about what would be the best mechanisms and measures at the national level to collect the information on “Beneficial ownership” (BO). He then explained about the FATF Recommendations on the “International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation” which provide the international standard to identify the risks and develop policies and domestic coordination to: pursue money laundering, terrorist financing and the financing of proliferation; apply preventive measures for the financial sector and other designated sectors; establish powers and responsibilities for the competent authorities and other institutional measures; enhance the transparency and availability of beneficial ownership information of legal persons and arrangements and to facilitate international cooperation.
Mr Rezy then referred to the FATF definition of BO which defines it as the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. He said it includes those natural persons who exercise ultimate effective control over a legal person or arrangement. He then discussed Recommendation 24 (transparency and beneficial ownership of legal persons) and Recommendation 25 (transparency and beneficial ownership of legal arrangements) of the FATF Forty Recommendations. Recommendation 24 stipulates that countries should take measures to prevent the misuse of legal persons for money laundering or terrorist financing. In contrast, Recommendation 25 states that countries should take measures to prevent the misuse of legal arrangements for money laundering or terrorist financing. Furthermore, countries should ensure that there is adequate, accurate and timely information on express trusts, including information on the settlor, trustee and the beneficiaries, that could be obtained or assessed in a timely fashion by the competent authorities.

The speaker later highlighted some relevant provisions under the Companies Act 1965 involving Section 69A on the furnishing of information and particulars of shareholding to the Registrar and Section 69O on the power of a company to require the disclosure of beneficial interests in its voting shares. He also mentioned: Section 131 on the disclosure of interests in contracts, property and offices; Section 134 on the registration of directors’ shareholdings and also Section 135 on the general duty to make a disclosure. Another statute he referred to was the Securities Industry (Central Depositories) Act 1991. He stated that under Section 2 of the Act, a “beneficial owner” of deposited securities is the ultimate owner of the deposited securities. This person is entitled to all rights, benefits, powers and privileges and is also subject to all liabilities, duties and obligations in respect of, or arising from, the deposited securities. However, a beneficial owner does not include a nominee of any description. Section 25(4) of the same Act stipulates that every account shall be in the name of the beneficial owner/authorised nominees, while under Section 25(5) it emphasises the declaration that he/she is the beneficial owner or authorised nominee of the said deposited securities.

Mr Rezy highlighted that the challenges in obtaining BO information were due to several factors including business efficacy and ease of doing business as opposed to any enforcement issue; the Central BO depository or regulatory environment; the lack of understanding of Customer Due Diligence (CDD) amongst corporate communities and company service providers; and issues on the accuracy and validation of BO information issues on the Personal Data Protection Act, with regards to personal data collected, particularly relating to the disclosure or the use of personal information.

He then ended his presentation by explaining the new Companies Bill under Clauses 56 and 50. The former clause relates to the power of a company to require the disclosure of the beneficial interest in its voting shares, which applies to all types of companies. In other words, this clause would enable a company to require a member to disclose to the company as to whether or not he holds the shares that are registered in the name of that member as a beneficial owner or a trustee. Also he explained that under Clause 56 the authorities can request similar information and it is an offence to disregard such a request. Clause 50 also provides for the duty to notify the particulars and changes in the
registers of the members. Under this Clause a company will have to notify the Registrar of any changes made regarding the shareholders in the register within 14 days from the date of the changes made. Failure to comply with the said provision is an offence and the company and its officers will be liable to a fine not exceeding RM20,000.

Nicky Antonius
Nicky Antonius, the third speaker, began his presentation by contending that the CDD was a weapon that could be used to verify the identity of the BO. He explained that with regards to CDD, the FATF Recommendations in 2012 focused on four questions as follows:

- **Who?** Verify identity of customer regardless of whether it is an individual or a company;
- **What?** The nature of business or employment of an individual;
- **How?** Most relevant to UBO is the ownership and control structure;
- **Why?** Assess and apply CDD to AML/CTF risks and also implement mitigations.

He then discussed the background and the context of the APG Typology Report received by the Financial Intelligence Units (FIUs) in the region. This report highlighted the top three common offences, which include tax-related offences fraud and smuggling and scams involving the cross-border transfer of funds. He then explained that entities such as shell companies, charities and offshore trusts could be used to channel money laundering and terrorism financing. For an example of shell companies, he explained that two companies were investigated by the New Zealand Financial Intelligence Unit. The first company was SP Trading Ltd, in which proceeds worth USD18 million were used to smuggle military weapons with an account based in Estonia. The second company was TERMED Ltd, which involved money laundering worth USD680 million for drug syndicates including the Sinaloa cartel.

Regarding charities, Antonius argued that the risks for charities in terms of UBO were quite relevant as could be seen from the APG Yearly Typology Report 2012. He identified several elements in terms of the vulnerabilities of charities as follows:

- The diversion of charitable contributions and use of own funds;
- A relatively low value of funds involved;
- Remittance to a high-risk country;
- The use of false names, but real telephone numbers.

With regards to offshore trust, he noted that there have been some indications of their vulnerability being used by criminals. These include criminals receiving funds as ‘loan drawn’ or in ‘advance’, international funds transfers to and from a high-risk jurisdictions, multiple high-value international funds for no apparent reason, and outgoing transfers followed soon after by incoming funds. On the tools to identify the BO, he suggested that some of the best practice tools were open source materials because of the impossibility of anticipating where the criminals might go next. He suggested making reference to the Overseas FIU Typology Reports, the APG Typology Report and also the AUSTRAC Report which provide effective guidelines for establishing, as well as identifying, the BO or customer identity.

The moderator concluded this concurrent session by saying that in operating in a global environment, there was a need to consider an international position regarding a standardised global policy and cross-border operation. Furthermore, he added that there will be challenges in determining UBO for complex
structures such as non-profit organisations for the purpose of CDD. The moderator also suggested that there must be an alternative approach on how to obtain information on the UBO. Rather than looking to local guidelines only, he suggested that it was important to consider international guidelines and the FATF Recommendations.

Q & A Session
During the question and answer session, several questions were raised by the audience and also by the moderator. The first question was whether there was any initiative to make a legal obligation for all companies to disclose all information pertaining to their BO. Mr Rezy responded by saying that there were challenges for both the regulators and also the stakeholders in creating the best mechanism to report to the enforcement agencies, including disclosing the UBO.

He also mentioned that at this time, there was no legal obligation mandating companies, shareholders and directors to disclose who their UBOs were. He highlighted that after the implementation of the new provisions of the Companies Act there would be some limitations on when a company requests information about the BO and when it wanted to know who was a trustee. He pointed out that in Malaysia companies were still figuring out the best mechanism of reporting, particularly in relation to BO. Even with the guidelines from the FATF Recommendations on BO, he observed that there was still a challenge in meeting the FATF Recommendations within the Malaysian AML regime.

The moderator then asked whether there would still be challenges if the new Companies Bill (Clause 56) was implemented. Mr Rezy responded by emphasising that even with the implementation of the revised Clause 56, there would still be challenges for local companies to declare the UBO. Furthermore, under Clause 56 it could be interpreted that it was not mandatory to disclose the BO. However, if the need arises, a company could request for the clause to apply.

The third question was posed to Mr Krishna, relating to the standard that was required in determining the UBO. Mr Krishna answered that in determining the UBO, it was based on an individual’s responsibilities on the account or account holder entity, his or her level of authority and influence over the account or account holder entity, and/or his or her vested ownership in the account asset or account holder entity, eg. not all Authorised Signatories may be UBOs as they may have limited control over the account. Therefore reliance may be placed on a Entity-level authorisation document such as a Board Resolution to determine who has a higher level of authority to be deemed as an UBO through direct control. He also mentioned that for other beneficial owners, the level of effective control was less than that exercised by the UBO.

However, he stated that a risk-based standard must be put in place as to what are acceptable independent sources for client-risk rating based, including applying potentially simplified due diligence where local law permits, to not have to determine UBOs companies rated lower risk such as where a company has a “listing on a reputable Stock Exchange”. However, for a client rated higher risk, even if listed, such cases could present some money laundering risks. In these instances, independent certification of ownership and management through functions that are expected to exercise entity-level oversight such as qualified accountants, legal professionals or auditors may be deemed appropriate.
CONCURRENT SESSION 2: International Perspective: (PEP)

Speakers:
Chrisol Correia  
Director, Global AML, LexisNexis Risk Solutions

Richard Chalmers  
Formerly, Co-Chair, Working Group on Evaluation and Implementation, Financial Action Task Force (FATF)

Eric A. Sohn  
CAM5, Director of Business Product, Dow Jones Risk & Compliance

Moderator:  
Rueben Panchadcharam  
Director, Financial Group, RHT Compliance Solutions

The moderator, Mr Panchadcharam, commenced the session by highlighting that the topic was something that was being looked at by compliance officers and boards of directors. Briefly he explained the broad contents of the session which would cover the requirement for Politically Exposed Person (PEP), and the practical approach and the challenges in dealing with PEP. He stressed that currently there was uncertainty around the issues of PEP, which need clarification.

Chrisol Correia, Director, Global AML, LexisNexis Risk Solutions

The first speaker, Mr Correia, began his presentation by highlighting that the issues of PEP were not new under the AML/CFT regime and had always been important within the compliance function. He then highlighted the global efforts in developing PEP standards such as those established by the United Nations, the FATF, the APG Group and also the OECD in their growing concerns over AML regulatory obligations.

Mr Correia said that when he first started his business back in 2001, there was no global understanding of the definition and roles of PEP. However, he noted that the FATF was the only organisation that had created a definition of PEP in its recommendations. The definition of PEP has gradually evolved to include foreign, domestic and any publicly known person. He quoted the Columbian experience in dealing with PEP in which a famous drug trafficker, a football player, and the well-known singer Shakira, have all been labelled as PEPs. Also the definition of PEP has been extended to cover family members of identified PEPs.

Mr Correia then discussed the challenges that could arise in the screening of PEP. One of these challenges is name matching, which is problematic, particularly, in screening client data against the watch lists. He contended that the high volume of data would require efficient throughput. The risk of overlooking a true hit must be balanced against the cost of reviewing excessive false positives. He noted that some of the records on national sanctions lists contained anomalies, while the lack of basic information such as a date of birth or even a surname could affect the screening process.

Mr Correia highlighted the difference between compliance effectiveness in contrast to the operational efficiency in PEP screening. He emphasised that the former was more concerned with the need to fulfil statutory obligations and to mitigate the risk of false positives. Meanwhile, the latter referred to the adoption of a risk-based approach (RBA) and resource-oriented measures in carrying out duties. He emphasised that there was a renewed interest in the RBA due to the on-going operational pressures and new regulatory requirements. The RBA was pertinent for institutions with large or diverse customer bases or high risk or high value products. Such an approach was more critical than before given the increasing regulatory interest in the implementation and maintenance of the RBA in compliance control systems. Another reason for the growing interest was the continuing need to consider RBA implementation across jurisdictions.

He suggested several risk factors to be considered for the RBA, involving the country of origin of the PEP, the national, regional or local type of PEP, the role of the PEP, the associations of the PEP, whether the PEP is active or passive, the domicile of the PEP – domestic or foreign, whether the PEP is alive or deceased, adverse media attention and the tenure of the role of the PEP. He suggested PEP risk assessments and a holistic view of client risk which would include age range, access to funds, legal events, professionals, personal associates, residency, geographic location, mobility and high risk news profiles and types. All these components would form the six main aspects of PEP screening involving the PEP or associates, sanctions/enforcement, connections, state organisation and adverse media.

Mr Correia concluded his presentation by highlighting the holistic benefits of adding the RBA into PEP screening. First, such an approach would streamline initial due diligence and on-boarding when a client opens an account. Second, it would enable organisations to prioritise alerts that acted as a quick means to identify areas to perform advanced due diligence. Third, the risk-based approach would help in the continuous monitoring of changes in life circumstances. Fourth, the RBA would decrease out of date due diligence information. Finally, the major benefit of adding the risk-based approach to the screening process was that it would reduce the cost of compliance within the organisation.
The second speaker, Mr Chalmers, began his presentation by thanking Mr Correia in highlighting the risk-based approach within the context of PEP screening. He then went on to look at the evolution of the definition PEP within the FATF context. He explained that the recent 2012 FATF standards extended the scope of PEPs to cover foreign PEPs, who were holding prominent public functions in foreign countries. He explained that domestic PEPs are those who hold similar positions in their own countries. Apart from foreign and domestic PEPs, the FATF also defined international PEPs to include senior management of international organisations. He added that in assessing all the above categories of PEPs, the adoption of a risk-based approach would be mandatory.

Mr Chalmers then discussed the extension of PEP by FATF. The first reason for this extension was due to the long-standing concern that corrupt PEPs would seek to hide stolen assets in foreign jurisdictions. Such concerns have led to the assumption that all foreign PEPs should be treated as high risks in relation to money laundering. The extension was mainly aimed at addressing the problem at the source, including concerns around denying financial services to PEPs and managing the political sensitivities in addressing this issue. The final reason behind the PEP extension was the concern about abuse within international bodies.

Mr Chalmers made special reference to the FATF 2013 guidance on identifying foreign and domestic PEPs. In assessing foreign PEPs, he referred to FATF Recommendation 12, which states that there is a need for an appropriate risk management system to be in place to determine whether the customer or beneficial owner is a foreign PEP. Such a system would require assessing customers through a risk-based approach, risk profiling, verification of CDD information and probably the institution’s own research into assessing the PEPs. In relation to domestic or international PEPs, again he quoted FATF Recommendation 12, which requires taking reasonable measures based on a risk assessment, as to whether the customer or the beneficial owner is a domestic PEP. Such measures would mean reviewing CDD data based on the relevant risk factors pursuant to FATF Recommendation 10, in order to determine whether the customer or beneficial owner is a domestic PEP. However, if the business risk is low, the issue of the customer being a PEP does not arise.

Mr Chalmers then posed a question on whether a person who has been categorised as a PEP should...
remain as one. He suggested that the labelling of PEPs depended on the particular factors and was based on the FATF Recommendation which indicated that usually a PEP’s labelling will be removed once he/she was out of office for a period of 12 months. However, the removal of PEP labelling would need to be evaluated using a risk-based approach due to the level of influence that the individual PEP might still possess and any links between the individual’s previous and current functions. He cautioned that institutions should monitor a PEP in order to determine whether that person was no longer a PEP.

On the rather difficult issue of PEP by association, he explained that there was no formal definition of “family members and close associates”. As such, he suggested that countries should provide some guidance and it would depend on the socio-economic and cultural structure of the country. Similarly, he contended that close associates or close connections could potentially be a broad grouping and could stem from political parties, trade unions, business interest and personal relationships outside the family. He believed that such persons should be treated as PEPs.

Mr Chalmers then pointed out that there was no universal risk-based approach that could be used in assessing PEPs and there is a need for on-going due diligence to identify the risk posed by them. Broader issues could also influence such CDD including country risks, political structure, economic structure, customer profiles and services.

In concluding his presentation, Mr Chalmers pointed out several challenges that could arise in identifying the risks posed by PEPs. Information sources and regularly updating the database, the baseline definition for being a PEP, identification of family members and associates, identification of beneficial ownership, influence and political pressure and influence of the PEPs group or state-owned entities, and the de-risking of PEPs, were among the challenges in regulating PEPs effectively.

Eric Sohn, CAMS, Director of Business Product, Dow Jones Risk & Compliance

Mr Sohn began his presentation by highlighting the need for the regulations since he was in the business of supplying effective prevention systems for money laundering. He said he agreed with Mr Correia in emphasising the importance of risk assessment measures within the AML/CTF system.

He then focused mainly on the challenges in dealings with PEPs. According to him, the first challenge was the definition of PEPs. He gave an example of Malaysian judges who could be possible PEPs. He suggested that sometimes a government officer could also be a criminal. He also stressed the importance of data in identifying PEPs. In this context, he referred to the differing naming practices in the US and China by way of example. In China, about 80 percent of the population have similar family names. This could mean any ordinary person being potentially identified as a PEP. In contrast, in the United States, only 20 percent of the population share the same last name.

He continued that the second challenge was the definition of foreign PEPs. He cited the FATF’s definition of a foreign PEP as someone who is entrusted with a prominent public role or function by a foreign country, such as the Head of State or government, senior politician, senior government officer, judge, military official or senior executive of state-owned corporations. However, he argued that the definition was vague.

In assessing the definition of PEPs, Mr Sohn described the problem of “a big fish in a small pond”. He believed that the treatment of all PEPs would not be the same and it could be different depending on the status of a person. He further stated that the “one size fits all” treatment would not work for all persons that could fall within the PEP category.

Mr Sohn then argued that corruption was the main offence linked to PEPs. He quoted the recent OECD Bribery Report in 2014, which revealed that the highest category of person who engaged in corruption were officers with government-linked companies (GLCs). Next on the list were heads of state, ministers and defence departments. Customs Department officers were also on the list of those linked with corruption.

Mr Sohn concluded his presentation by looking at the way forward when dealing with PEPs. He advised that in assessing PEPs, consideration should be given to the job held and the likelihood of the officer’s involvement in crime and, finally, every decision and preventive measure taken by an organisation in dealing with PEPs should be documented to ensure an effective and efficient PEPs monitoring programme.

Q & A Session

During the question and answer session, the speakers responded to the first question raised by the moderator as to what appropriate measures should be taken if a PEP were a company and not a person. Mr Correia said that it was necessary to adopt some way of assessing the relationship
between the company and the PEPs concerned. Mr Sohn agreed with Mr Correia that in assessing companies as a PEP consideration should be given to the risk-based approach and that all mitigation measures and plans should be documented properly. Mr Chalmers added that if a company was a PEP, it would be necessary to look into the level of influence either from shareholders or the board of directors.

The second question related to FATF Recommendation 12 which mentions the identification of PEPs and the requirement for approval by senior management to retain customers who are suspected of being PEPs. Given this, the question was to what extent could financial institutions rely solely on the database provided by service providers especially since most financial institutions are relying on the same database. The question was also extended to include how the regulators view the databases provided by service providers. In response, Mr Correia stated that in assessing PEPs it was crucial for financial institutions to adopt a risk-based approach and it was up to the organisation to assess their respective customers. Mr Chalmers added that the databases provided by service providers were helpful but could be deficient to some extent. In mitigating this situation, he advised that institutions look at the nature of the business and the jurisdiction in which the PEPs are domiciled. He then gave an example that if a non-resident wanted to have a banking facility, then enhanced due diligence should be exercised as there was a threat of potential abuse. On the same question, Mr Sohn replied that the institutions concerned should conduct their due diligence process and that the database was not the total solution.

The final question related to the status of GovernmentLinked Companies (GLCs) and state-owned enterprises, since these two entities were exempted from due diligence and were declared as not posing any risk to money laundering and terrorism financing. Mr Chalmers responded to the question by saying that it was well recognised that GLCs posed a low risk of such crimes. However, he added that there was a need to look into individual GLCs when there were concerns for potential abuse. He added that GLCs have a high tendency for corruption. In dealing with GLCs, it should be noted that the concern was more with individuals rather than the company. In answering this particular question, Mr Sohn stood by his earlier views that financial institutions should be more cautious when dealing with GLCs due to the potential for corruption.
PLENARY SESSION 3:

The Way Forward: Adapting to Change in Compliance

Speakers:

Tyrone Cole
Senior Solutions Consultant, BAE Systems Applied Intelligence

Vijayakumar MV Nair
Deputy Director, Financial Conglomerates Supervision, Bank Negara Malaysia

Moderator:

Sam Gibbins
General Manager, Asia, GRC Solutions

Tyrone Cole, Senior Solutions Consultant, BAE Systems Applied Intelligence

The first speaker, Mr Cole, began his presentation by thanking the organisers for giving him the opportunity to be one of the speakers at the conference. He pointed out that his presentation entitled, “Data Sharing: Motivation and Incentives” would cover how data could be used within an organisation to better understand the risks involved. Also, he would discuss how data could be used to establish a working collaboration between institutions and database providers in fighting against financial crimes.

Next, Mr Cole discussed who would want to share their data. He stated that previously, only organisations which wanted to share data were limited to banking, government, and the insurance sector. Today, the list has been expanded to include the energy, health, telecommunications and e-commerce sectors. He added that the rationale for sharing data includes the need for regulators and system providers to match the data sharing of criminals in this modern, digitally enhanced world. Sharing data would be mutually beneficial in defending organisations against attack and working together to fight financial crimes would be more effective than working alone. He explained the critical factors that were enabling data sharing: the high proportion of data owners able to take part; the fact that data sharing is good value for money as the returns could be quantified; improved organisational agility in adapting to changing threats; and data availability. Sharing was not limited to data but could be extended to the sharing of operational costs, technology deployment and expertise to identify new threats.

Mr Cole then focused on types of data, which he divided into three conceptual categories of “known bad” data, “grey” data and “all” data. However, he thought that defining such data was hard to do for the whole industry. New technologies are allowing easier processing of big data. He also thought that sharing all data would avoid bias towards the types of fraud found in a single organisation.

Mr Cole then discussed approaches to the sharing of intelligence that included legislation, club and commercial types of sharing. Each type of intelligence sharing had its problems and consequences. Mr Cole provided three case studies to illustrate each type of approach. On the pitfalls of data sharing, he believed that an additional intelligence system would not replace the local systems and there was a trade-off to be made between data volumes and control. He stated that the perils of personal information would include the fear of bad media coverage in terms of “big brother databases”, ambiguous regulation, as well as the risks of cyber-attack and data loss.

In conclusion, Mr Cole emphasised that with the growing sophistication and organisation of criminals, there was a necessity to share data. Also, there was a need to work together to understand business partners and for utilising the right information in the right context for accurate, quick and confident decisions. Lastly, he argued that data sharing was important to facilitate further understanding of the risks in any organisation.

Vijayakumar MV Nair, Deputy Director, Financial Conglomerates Supervision, Bank Negara Malaysia

The second speaker, Mr Nair, began his presentation on supervisory views of the compliance function. He stressed that within the compliance function, risk management and a risk-based approach were important in order to carry out the function effectively. Mr Nair then argued that with the development of the compliance function, the Central Bank had issued guidelines and standards to assist the financial sectors and non-financial sectors covered under the AML regime. He added in jest that financial criminals seemed to be always ahead of the regulators and appear to be employing good risk management techniques themselves to avoid detection. He suggested that financial institutions should also...
enhance their own approaches to detect activities that could facilitate ML/TF. Also, he contended that the risk management approach was focused on identifying the gaps in the current system, which could be vulnerable to criminals.

Next Mr Nair emphasised that failure to manage compliance risks within financial institutions could result in penalties being imposed by the regulators, reputational concerns for the respective financial institution, and the role of financial institutions generally which, in turn, could affect the country’s economy as a whole.

In overseeing the effectiveness of the compliance function, Mr Nair stressed that the Chief Compliance Officer should get everyone involved in the organisation, including senior management and frontline staff. Such involvement was crucial and to facilitate this the first thing that should be in place in terms of achieving compliance was the right compliance framework and internal controls.

Mr Nair continued by advising that the role of financial institutions should be more proactive rather than passively waiting for the Central Bank to issue guidelines. Furthermore, he said that compliance nowadays was no longer a “tick box” approach but rather taking pre-emptive steps that require intelligence, technology and human intervention in order to make the compliance function successful.

Mr Nair concluded his presentation by advising that all financial institutions should play a proactive role in ensuring compliance. Furthermore, he added that it would be better if the AML/CFT regime underwent periodical reviews so as to ensure it could cater for the current financial crime threats and trends facing financial institutions.
Q & A Session

During the question and answer session the speakers responded to the first question raised by the moderator on what action could be taken to reduce negative feedback from the public on data sharing and the practicality of club data sharing in Malaysia. Mr Cole responded that there was a negative perception regarding this. However, the purpose of sharing needed to be clarified so as to prevent the greater harm of criminal activities taking place. The sharing of data could also send a positive message about the institutions themselves. On the practicality of the club data sharing, Mr Cole responded that such an approach could work in Malaysia as there was a need to better assess the country’s vulnerabilities to such crimes and the NGOs could be in a better position to share data.

The second question from the moderator was posed to Mr Nair on how to change the perception of the working culture of compliance officers within the industry. Mr Nair replied that historically compliance was considered as the last thing to look into by the financial institutions. Non-compliance could trigger many issues within financial institutions such as reputational risk as a result of penalties or loss of confidence by the depositors and investors. Mr Nair reiterated that compliance function was no longer a “tick box” approach, and it needed involvement from top management and the board to oversee the important underlying message contained within it, since a compliance failure could put financial institutions in a difficult situation.

The third question from the audience was on how various jurisdictions found ways of sharing data and how the problem of the Bank Secrecy Act and personal data protection law be managed within the data sharing process. Mr Nair answered that within the industry there should be a mutually recognised level of practice to enable data sharing more effectively.

The fourth question was about the perception of database solution providers on issues of ethical data acquisition and sharing as some information could be sensitive to a particular institution and it could not be independently verified. Mr Cole replied that in considering ethical data sharing and acquisition, it should be based on each participating member and what their standards of personal data were. The database service providers would always try to localise their services to the country’s need.

The fifth question from the moderator to Mr Nair was on the role of technology in assisting AML compliance. He responded that technology was a vital part in the AML/ CFT measures as it would transform data into information that could be used by the regulators. The sixth question was put to Mr Cole on the future of clients’ needs in relation to the advancement of technology. He was also asked about the way in which financial crime technology providers would cater to such needs. Mr Cole answered that periodic optimisation of efficiency is becoming more and more of a focus for regulators, technology plays a significant part in enabling this change. Such initiatives to adopt technology to support optimisation processes could serve as evidence to the regulators on the efforts taken and progress made by the particular institute.

The seventh question from a member of the floor was on the manner of data loss protection and what methods to prevent leakage of data being shared could be adopted. Mr Cole replied that data loss protection formed part of a wider network security process that can be mitigated with enterprise defence solutions.

The final question was posed to Mr Nair about regulatory perspectives on the way in which robust controls on the growing threats of financial crimes and that critical data sharing could happen. He replied that the idea of putting a robust system in place came with some legal impediments. Furthermore, he agreed with Mr Cole’s views on anonymous data sharing and the need to create a proper channel to share such data.
The moderator began the session by highlighting the need to improve the skills of compliance officers and the overall compliance function within organisations. The session focused on the issue of talent shortages in the compliance function and possible solutions to the issue. The global financial crisis has increased the focus on regulation and risk management which has led to an increase in the demand for compliance professionals. However, negative perceptions associated with the compliance profession have resulted in compliance roles not being seen as being as attractive as other roles.

Dr Wan Nursofiza Wan Azmi, Director, Strategy, Policy Development & Research, Asian Institute of Finance

Dr Wan Nursofiza emphasised that compliance and risk management became a major issue following the global financial crisis. Organisations, particularly those in the financial services industry were facing challenges in recruiting and retaining skilled staff. She referred to the AIF survey in 2014 on talent shortage in the financial services industry. Results from the survey showed about 76 percent of the employers in the financial services industry were facing talent shortages and had difficulties in hiring risk and compliance officers due to increased compliance requirements.
She contended that compliance and risk management officers must have good leadership skills and possess high emotional intelligence quotients (EQ) to be effective in advising and influencing the senior management and board members. She then suggested that the solutions undertaken by organisations in overcoming talent shortages could include promoting talents internally, providing training for up-skilling, and developing effective succession planning. As risk management and compliance positions were not viewed as attractive roles, Dr Wan Nursofiza suggested attracting the younger generation to fill in the gaps by giving greater consideration to their preferences.

Nicky Antonius

Antonius shared his perspectives on talent. He said that talent was better addressed based in terms of teams instead of individuals. A good and talented team should be proactive in coming up with new ideas and seeking new ways to perform their functions. The team should consist of diverse skill sets while working on two different streams: a few members performing regular tasks while the rest worked on experimental tasks to expand their knowledge of new concepts. He cited Google Inc. as using this method and it was proven to be successful because employees were able to come up with new ideas and suggestions for different projects.

He then argued that there should also be a clear progression pathway for the team to look forward to when performing their tasks. A good team needs to have knowledge and understanding of compliance, data sciences knowledge, and be capable of good initiatives. These three elements must exist in establishing a competent compliance team.

Also he argued that organisations should implement self-service compliance. The compliance function in an organisation cannot be based on the compliance officers alone. Instead, compliance officers should focus more on complex compliance tasks while others could undertake the simpler compliance tasks in the
organisation. Compliance knowledge, frameworks and processes should be shared across the organisation to create compliance awareness among the employees. Therefore, everyone in the organisation has a responsibility to ensure compliance.

Nora Manaf, Group Chief Human Capital Officer, Maybank Group
Ms Manaf next shared her views from a human resources perspective. She agreed with both the previous speakers and stated that compliance officers should have both technical and soft skills. She emphasised that good communication had become very important. She said that the perception of others would not change with a change of name: it was dependent on the outcome and contribution of an action. Ms Manaf added that most compliance officers came from within the organisation because of their organisational knowledge and network.

Closer to home, she explained that Maybank only recruited high potential candidates. The expectation placed on employees was high and employees must ensure that the resources spent by the organisation were value for money. Therefore, employees must ensure that their capability and quality must be consistent with the salary offered.

Q & A Session
During the Q & A session, an audience member raised an issue on the importance of strategic thinking among compliance officers and the need to fully utilise the available resources. All speakers agreed that both technical and soft skills were very important for compliance officers. Antonius emphasised that technical skills could be learned, but good communication skills would make a person more outstanding than others. Also he mentioned that there was a need for strategic thinking that focused on knowing about the organisation’s future direction and the responsibility of each component of the organisation. There should be an extensive organisational network able to identify issues impacting across it and able to identify solutions to potential problems.

To deal with the talent crisis, Dr Wan Nursofiza stressed approaching this issue from an industry-wide perspective by having a workable industry-wide competency framework. The result of a survey conducted by AIF indicated the need for a clear career path for the financial services industry. Having clear career paths, would attract more capable people to join the financial services industry and this would subsequently overcome the issue of recruiting and retaining talented employees. AIF proposed the construction of a clear industry-wide competency framework covering all four financial services sectors. The framework should allow employees to move between sectors for better career development while providing an enjoyable learning experience.

Mr Neil Smith delivered the closing points of the session by concluding that it was important for compliance officers to have both technical and soft skills and that having a clear career path would increase the attractiveness of the compliance function.
CONCURRENT SESSION 3:

Integration of National Risk Assessment (NRA) with the Banks’ Risk Assessment

Speakers:
Zarifa Izan Zainol Abidin
Deputy Director, Financial Intelligence and Enforcement Department, Bank Negara Malaysia

Michael McGillion
Manager, National Security Operations, Australian Transaction Reports and Analysis Centre (AUSTRAC)

B.C. Tan
Head of Research, Asia Pacific, Thomson Reuters

Moderator:
Samsudin Samsuri
Country AML/CFT Compliance Head, UOB Bank Malaysia

Mr. Samsudin began the session by outlining three important questions that needed to be addressed by the speakers during their presentations. The first question dealt with defining the National Risk Assessment (NRA) followed by how NRA could be integrated into the development of AML/CFT in organisations and lastly how the implementation of AML/CFT itself was being implemented in organisations.

Zarifa Izan Zainol Abidin
Deputy Director, Financial Intelligence and Enforcement Department, Bank Negara Malaysia

The first speaker, Ms. Zarifa Izan, began her presentation by giving an overview of NRA from the perspective of the regulators using the results of the NRA in 2013. She outlined three main key points. First, the NRA was one of the tools to facilitate AML/CFT risk assessment and it was an ongoing process as risk is unpredictable. Second, reporting institutions should identify the AML/CFT risks such as understanding the customer’s behaviour including both domestic and foreign. Finally, reporting institutions should incorporate the results of the NRA into the organisation for the wider assessment of the risks identified by the organisation.

Ms. Zarifa further stated that the data analysed in the NRA comprised statistical data, opinion surveys, international reports and expert
views, all of which provided crucial information that could be relied upon by the users. Based on the analysis employed, it was shown that the five types of crimes which had a high incidence in Malaysia were fraud, drug trafficking, corruption and bribery, smuggling and tax crimes, all of which generated large illicit proceeds. She also stated that three main sectors that were highly vulnerable to money laundering are banking, money service providers and casinos. The country’s structural elements such as economic, geographical and legal frameworks influence the prevalence of crimes and sectoral vulnerabilities.

She pointed out that the results from the NRA could be applied to the risk assessment of an organisation in two classifications - high-risk sectors and prevailing crimes. She argued that it was crucial to treat the sector and its customers and transactions as risk indicators. Meanwhile, other factors that needed to be considered in measuring susceptibility to the prevailing crimes were the susceptibility of the sector and its customers, products and services, geographical coverage and delivery channels.

Ms Zarifa concluded her presentation by emphasising that having complete knowledge of the nature and the extent of threats and how they could happen would assist in risk mitigation. Also she argued that risk assessment did not have to be complex. Instead it should be commensurate with the nature and size of the bank’s business. Banks should also complement their assessment with other relevant internal sources (such as reports from heads of business and relationship managers) and external sources (such as the NRA and typologies).

Michael McGillion, Manager, National Security Operations, Australian Transaction Reports and Analysis Centre (AUSTRAC)

Mr McGillion began his presentation by highlighting some of the limitations of applying the NRA to an organisation’s risk assessment. The first limitations was due to the timeliness of the NRA. In essence, by the time it hits the surface, the data received could be obsolete. He therefore argued that such an assessment should be complemented

"Based on the analysis employed, it was shown that the five types of crimes which had a high incidence in Malaysia were fraud, drug trafficking, corruption and bribery, smuggling and tax crimes.

Zarifa Izan Zainol Abidin"
by additional information such as regular updates on the typologies and sharing of information between banks to ensure their risk assessment was up-to-date. He argued that the second limitation was the scope and purpose of the NRA. Currently the NRA is mainly for government agencies. As such, the conflict between the scope of government agencies and that of multi-national corporations might lead to ineffectiveness in establishing the context that would fit the organisation.

To overcome this, Mr McGillion suggested that corporations should spend more time and effort to develop trust with law enforcement agencies. They should demonstrate value to the law enforcement agencies so that such agencies would engage with corporations in the working process. Close cooperation with law enforcement provides a valuable source of information that helps inform risk assessment. Also, providing greater support to the law enforcement agencies can be a powerful demonstration of the effectiveness of compliance processes to the regulator.

**B.C. Tan, Head of Research, Asia Pacific, Thomson Reuters**

The final speaker, Mr Tan, ended this concurrent session by highlighting the trigger points of compliance issues and their links with risk assessment for the NRA. From a survey conducted by Thomson Reuters, it was found that compliance teams were spending more than seven hours per week amending policies and procedures to reflect the latest regulatory rules. He stated that spending more money on compliance issues did not necessarily improve the situation. He stated that it was best to shift from the old compliance approach to the dynamic risk-based approach. He believed that the results of the NRA, whatever its scope, could also provide useful information to financial institutions and designated non-financial businesses and professions (DNFBPs) to support their risk assessments.

Mr Tan suggested that both qualitative and quantitative approaches are needed in conducting risk assessments. A qualitative approach would help to identify and contextualise the risks faced by organisations. It could also help to profile the risks and identify the risk appetite of corporations. It would give credibility to the assessment as well as enable scenario planning. He suggested that one of the sources for data was through stakeholders since they were more familiar with the particular situation of a corporation. However, he warned that the qualitative approach is limited to understanding the scenarios. To operationalise risk assessment, a quantitative approach must be adopted. This approach could help to assess, measure and report the risk exposure. It would be useful regarding rule setting and it would also provide the red flag indicators for organisations.

He concluded his presentation by suggesting that for future risk-based implementation, organisations should identify the risks they might face and build a risk assessment programme that was scalable with long-term continuity. Such a programme must be continually maintained, be made part of the decision-making process and should also be measurable.

Mr Samsudin Samsuri ended the session by concluding that the NRA complemented the risk-based approach.
CONCURRENT SESSION 4:
Crime Trends in Malaysia and Combating Money Laundering

Speaker:
Dato’ Akhbar Satar
Founder and President, Association of Certified Fraud Examiners (ACFE) Malaysia Chapter

DSP Mohd Noor Firdauz Abdullah
AMLA Senior Investigating Officer, Commercial Crime Investigation Department, Royal Malaysia Police

Mohamad Shariff Bin Atip
Senior Assistant Director, Customs

Md Fahmi Bin Md Said
Principal Assistant Director, Inland Revenue Board of Malaysia (IRBM)

Moderator:
Mohd Fuad Arshad
Deputy Director, Financial Intelligence and Enforcement Department, Bank Negara Malaysia

The moderator commenced the session by giving a broad overview of the discussion topic of “Crime Trends and Combating Money Laundering in Malaysia”. He stated that this session would focus on the emerging trends of financial crime. He believed that in the context of risk management it was very relevant to the financial industry to keep up to date with the continuously changing complexity of financial crime. However, he noted that the challenges were due to the lack of expertise and knowledge regarding financial crime. The moderator highlighted that the role of Bank Negara as a regulatory body was to keep abreast of the changing development in financial crime as well as sharing information and assisting financial institutions and law enforcement agencies in understanding the risks of such crime. Such a role could help in risk assessment initiatives inside and outside financial institutions.

Dato’ Akhbar Satar, the first speaker, started his presentation by showing the results of the recent National Risk Assessment 2015 in Malaysia. He stated that the level of threat of money laundering in Malaysia had increased with fraud in particular as a risk. He explained that there was no specific definition of fraud and highlighted that the broad category of fraud could include cheating, theft and criminal breach of trust. Also he highlighted that there were various types of fraud including e-banking fraud, credit card fraud, inheritance fraud, parcel scams, insurance fraud and international fraud. He added that currently in the USA fraud was categorised as a serious crime. Other high-risk crimes were drug trafficking, smuggling, tax crimes as well as corruption and bribery. Terrorism and terrorist financing were considered as medium risk crimes.

Dato’ Akhbar then highlighted that according to Price Waterhouse’s Global Economic Crime Survey in 2014, cybercrime has emerged as the most popular type of economic crime in Malaysia and has surpassed drug trafficking as being the most lucrative. He quoted statistics from the Royal Malaysian Police that showed about 70 percent of commercial crime cases were categorised as cybercrime. He further added that the threat of cyber terrorism included attacks against Critical National ICT Infrastructure, the spread of militant political propaganda and even the recruitment of potential members into terrorist groups. He gave the example of America and Israel damaging the Iranian nuclear control system that could be considered as an act of cyber war.

Dato’ Akhbar discussed drug smuggling next. He explained that Syabu could be categorised as a drug and that it could be imported from Iran at a cheaper price. He pointed out that most of the drug smuggling cases were difficult to detect. However, in 2014, the Royal Malaysia Police confiscated drugs from smuggling activities worth RM2.5 million. He urged Malaysians to be thankful to the police as the job of preventing drug smuggling was not an easy task. Dato’ Akhbar then mentioned human trafficking. He quoted the recent situation at the Malaysia-Thailand border where the police had discovered a human trafficking camp in the forest.

Next he discussed arms smuggling. He pointed out that the US government had put in place a software system that could easily detect arms smuggling. However, the situation was different in Malaysia whereby 80 percent of cases of arms smuggling were difficult to detect due to the lack of integrity of the law enforcement. He emphasised that the integrity factor was very important and that Malaysians must be educated from an early age about this value.

Dato’ Akhbar then identified prostitution as the sixth key crime. He explained that, according to unofficial reports, there were around 150,000 prostitutes in Malaysia, with about 10,000 to 20,000 of them in the Klang Valley. He was disappointed with the claims that the problem was due to the absence of integrity among the law enforcement agencies.

Another crime that he focused on was tobacco smuggling. The illicit cigarette trade was one of the most attractive options for funding organised crimes and terrorist activities. He mentioned the fact that Malaysians smoked 23 billion sticks of cigarettes, out of which 8 billion sticks were contraband. He claimed that some
influential people were involved in tobacco smuggling. The country lost approximately RM2 billion of revenue to tobacco smuggling which led him to conclude that there was high demand, high profits and low penalties for such crimes.

Dato’ Akhbar then made special reference to the corruption perception index in Malaysia. In 2014 the index showed that Malaysia ranked 50 out of 175 countries globally. The index also revealed that 45 percent of corruption cases involved political parties.

On terrorism he stated that in assessing its definition, the term terrorism was not universally accepted due to various significant political, religious and national implications. He observed that the primary objectives of terrorism were to intimidate a population and to compel a government or international organisation to commit to, or abstain from an act.

Dato’ Akhbar went on to define terrorism financing as a process of financing terrorist activities either through legitimate sources such as donations or illegitimate sources such as drug trafficking and corruption. He disclosed that according to the Global Terrorism Index in 2014, Malaysia ranked 48. The sources of funds for terrorist financing included: ‘donations’, investments, as well as individual and extralegal activities.

Dato’ Akhbar continued his presentation by defining money laundering. According to him, money laundering was a process of converting cash or property derived from criminal activities to give it a legitimate appearance. It was a process to clean dirty money to disguise its criminal origin. He further explained that there were three stages of money laundering: placement, layering and integration.

He then analysed the differences between money laundering and terrorist financing. First, the motivation for the former is profit, while the motivation for the latter crime is ideology. Second, the funds for money laundering are derived from numerous crimes whereas funds for terrorist financing originate from donations, business, sponsorship and crime. Third, the modus operandi of money laundering is the laundering of dirty money, while ‘clean’ money may also be involved in terrorist financing.

Fourth, money laundering could be committed within the formal financial system, while terrorist financing as a hidden crime would usually be committed within the informal financial system. Fifth, in money laundering cases the funds would enter the legitimate economy, whereas the funds involved in terrorist financing would inevitably be channelled to terrorist organisations.

He then suggested several ways in which money laundering could be prevented including effective law enforcement; fighting its predicate offences such as corruption, terrorism and cybercrime; increased intelligence gathering; international cooperation; screening people with access to sensitive information, and checking the integrity of law enforcement and regulatory bodies.

Dato’ Akhbar ended his session by emphasising the importance of integrity in fighting against crimes such as corruption, drug trafficking, prostitution and other crimes. The education system should play an active role by installing moral values such as integrity within the financial system. He stressed that members of society must adhere to the regulations of the country.

DSP Mohd Noor Firdauz Abdullah, AMLA Senior Investigating Officer, Commercial Crime Investigation Department, Royal Malaysia Police

The second speaker, DSP Mohd Noor Firdauz, highlighted that as the crime of money laundering generated significant profits for the criminals it might in turn create a “need” for money laundering. He stated that organised crime and financial crime in Malaysia had caused RM15-25 billion of losses every year which could undermine the integrity of the financial system. He illustrated the case of American States v Kramer in which the court held that the essence of money laundering was deceit and “cover-up” and it would normally involve a highly complex process.

Dwelling on the issue of money laundering, he identified that the motives were: firstly, to remove or distance the illegal proceeds from the perpetrator which would make it difficult to detect and to prosecute him/her; second, to prevent the illegal proceeds from being confiscated; third, to enable the criminal to enjoy the benefits of the illegal proceeds without being detected; and lastly, to reinvest criminal proceeds into future criminal activity or business, either legal or illegal.

DSP Mohd Noor Firdauz then discussed the perspectives of the law enforcement agency on money laundering. There were four questions to consider including the nature of the transaction, the origin of the money, the knowledge of the launderer that the money was “dirty” and the criminal’s dealings with the money.

He then examined the linkages between money laundering and the banking sector. He described banking as the most popular sector to generate an opportunity for criminals to launder dirty money by criminals. He then explained that there were several
ways to launder money through the banking sector. Firstly, criminals could misuse a bank account. Secondly, there was international fund transfers where money could be moved rapidly and securely across borders. Thirdly, there were loans, where the laundering proceeds could be hidden under the guise of repayment. Finally, the bearer of negotiable instruments (BNI) such as bank drafts, promissory notes, traveller’s cheques and money orders, could be used to launder illegal proceeds.

DSP Mohd Noor Firdauz also discussed the first money laundering case in Malaysia, that of Dr Hamimah, where RM42 million loans were obtained and released to Dana Harta. The suspect then conspired with three bankers who falsified bank documents. The money from Dana Harta was transferred to several companies owned by the suspect who purchased six cashier orders under the company profiles. The suspect was found guilty and sentenced to eight years imprisonment.

He then indicated that another method commonly used by the criminals to launder illicit gains is through remittances services. Transferring money without actual movement is known as “hawala” in Malaysia. He explained that such a method would involve some financial debit-credit “offsetting”. Next he observed that money laundering could also be linked to the gaming sector. DSP Mohd Noor Firdauz mentioned that criminals exchanged illegal proceeds with casino chips and later on claimed them as winnings.
Trade finance now poses a very high risk and the processes involved are vulnerable to abuse.

Mohamad Shariff Bin Atip

In concluding his presentation, DSP Mohd Noor Firdauz demonstrated that the challenges of money laundering crimes were due to several factors. Firstly, a new method of money laundering had evolved in the wake of September 11, 2001, when funds from The United Arab Emirates were transferred to various banks in New York. Secondly, mutual legal assistance through collaboration and networking was rather difficult. Here he suggested that law enforcement agencies and the financial institutions must cooperate more for the purpose of gathering and exchanging information. Third, there was a lack of robust implementation of policy for international sanctions.

Mohamad Shariff Bin Atip, Senior Assistant Director, Customs

The third speaker, Mr Mohamad Shariff, started his presentation by highlighting offences investigated by the Customs Department which, he believed, would be unfamiliar to most of the audience. He then described a classic Customs offence relating to the importation of fruits from the US in which Customs issued two invoices to two parties, one being the owner of the goods and the other the importer. The full amount was RM26,000 which was divided in two so that each party would obtain RM13,000 and as a result less tax was paid. From that example he demonstrated how easy it was to manipulate invoices and taxes.

He then explained that the primary basis for customs value under the WTO Customs Valuation Agreement was transaction value. He further explained that many Customs administrations applied the transaction value method to more than 90 percent of their imports. As such, the alternative value method was only used when it was not possible to establish a transaction value.

Mr Mohamad Shariff then identified the various methods used in committing customs offences. For example, the creation of duplicate invoices for a single trade transaction; invoicing the same goods more than once for the same shipment would allow the value to be moved through multiple payments; and payments could be disguised by using different financial institutions. Even if the law enforcement agency was able to detect multiple payments there could be legitimate explanations, including corrections or amendments to the payments.

He then examined the current trends in tax crimes from the Royal Malaysian Customs typology studies. He identified clear evidence of criminal organisations exploiting the vulnerabilities in the international trade system to move funds for illegal purposes. Trade finance had become the main concern to the Customs Department due to the red flags of the risks involved. Consequently, trade finance now poses a very high risk and the processes involved are vulnerable to abuse. Trade finance is being used to obscure the illegal movement of funds through misrepresenting the price, quality or quantity of the goods. He noted that the proceeds of fraud from tax crimes had been used to finance the trade itself.

According to Mr Mohamad Shariff, the most common fraudulent trade practices in recent times were the under-invoicing of goods, double-invoicing and multiple invoicing. In these situations, a complex web of transactions and movements of goods typically occurred. The payment could be disguised by using multiple transactions through various financial institutions. There had also been cases of collusion between sellers and buyers as a result of open account financing i.e. the open account commonly used between established and trusted traders for that particular transaction. Both parties to the transaction could be controlled by the same person.

He then described how financial institutions could identify red flags for tax crimes in the following circumstances:

• The payment for goods is more than the known market value;
• The payment for goods is below the known market value;
• Discrepancies in the shipping documents;
• The products or options do not correspond to the line of business;
• The shipment is purchased by firms or individuals from foreign countries other than the country of the stated end user;
• The letter of credit transaction is awaiting approval by the new account;
• The parties on the letter of credit do not appear to have any obvious relationship or connection to the underlying transaction;
• The frequent modification of the letter of credit making it unnecessarily complicated for no apparent legitimate reason;
• Wire instructions or payment from or due to parties who are not identified in the original letter of credit;
• Wire transfer activity that is unexplained, repetitive or shows unusual patterns;
• Transfer of funds or wires to the other accounts held by the customer for no apparent reason;
• The transaction involves the use of shell companies;
• The exporter’s account shows the activity of previous wire transfer activity from countries of concern or business unrelated to the stated business activity.

In conclusion, he observed that Customs relied on the capacity of the financial institutions to identify anomalies. Mr Mohamad Shariff noted
that the RMC needed to cooperate with the FIUs. He also noted that the current level of international cooperation among FIUs was possible through the Egmont Secure Web.

Md Fahmi Bin Md Said, Principal Assistant Director, Inland Revenue Board of Malaysia (IRBM)
The last speaker, Mr Md Fahmi, started his presentation by talking about the case of a football player, Lionel Messi, who was charged with tax offences in June 2015. Later, his father who was also his manager, was prosecuted for the fraudulent offences. He therefore showed that tax evasion was not only a predicate offence under the AMLA 2001, but was also an important issue at the international level.

In Malaysia, tax evasion falls under Schedule II of the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLA). Tuan Md Fahmi also emphasised the relevant offences under the Income Tax Act 1967 such as Section 112 on the failure to furnish returns, Section 113 of the same Act regarding filing of incorrect returns and Section 114 that provides for wilful evasion.

He emphasised that according to the National Risk Assessment 2015, tax evasion was the most important high risk offence. Other high risk crimes include fraud, drug trafficking, smuggling and corruption. He explained that the effect of these offences could have an adverse impact on the economic development of the country.
Mr Md Fahmi then highlighted the crime trends in money laundering. Firstly, money laundering typically involved cross-border transactions, in which more than one country might be involved. Secondly, the criminals tend to create organised crimes with other professionals such as accountants, lawyers and tax consultants. Thirdly, the advancement of technology provided an opportunity for the criminals to communicate easily online. Fourthly, businesses were mainly registered under nominees most of whom were the sole proprietor of the company. The business could also involve many related parties such as family members or close friends to disguise the criminal activities. Fifthly, the most favourable method to transfer the money was via the alternative remittance system also known as “hawala”. Lastly, was a fraudulent tax scheme popular among big companies that applied final status (income exempted from tax) – once the status expired, the company then renewed its application using the name of other companies.

He proposed several initiatives to combat tax evasion and money laundering such as through cooperation with law enforcement agencies; international cooperation; strengthening of the workforce or capacity building; strengthening the tax laws; enhancing information and communication technology.

Mr Md Fahmi concluded his presentation with the advice to participants to take their responsibilities seriously. He also suggested that as professionals, they should uphold strong moral principles and integrity to counter tax crimes for the benefit of the next generation.

Q & A Session
During the question and answer session, the first question posed to the panellists was to get their views on the complexity of financial crimes in Malaysia over the next ten years. Dato’ Akhbar responded that the crime rate had increased along with population growth. He added that as technology had developed and increased, cybercrime became the cost effective method to make money.

The second question was related to money laundering and terrorist financing and on how, in particular, to obtain the lists of convicted criminals from the Royal Malaysia Police. DSP Mohd Noor Firdaus replied to the question by stating that they have set up a unit with a specialised officer in charge to deal with requests for criminal information and records. Information would be provided on a case by case basis, but was subject to private and confidential information rules. He explained that the stated procedures i.e. to request the information in a letter and submit it to the counter-terrorism Department in Bukit Aman must be followed.

The third question was concerned with the issue of human trafficking or smuggling. Dato’ Akhbar responded by saying that it was necessary to look at the issues behind the scenes. This crime was committed due to corruption and its deterrence requires the government to take measures and initiatives to avoid corruption in the country.

The final question was on measures to improve financial institutions and law enforcement in preventing money laundering and tax crimes. Mr Shariff replied by stating that it was imperative to establish cooperation and networking between the financial institutions and law enforcement. Compliance officers must be contacted about any problems arising so that they could be addressed and solved as quickly as possible.
PLENARY SESSION 5:
Terrorist Financing, ISIS and Sanctions

Speaker: SA Robert Josh Williamson
Special Agent, FBI Legal Attaché Office Manila, Philippines

Dr Muhammad Yusuf
Head, Indonesian Financial Transaction Reports and Analysis Centre (PPATK)

Michael McGillion
Manager, National Security Operations, Australian Transaction Reports & Analysis Centre (AUSTRAC)

Moderator: DSP Foo Wei Min
Deputy Superintendent of Police, Royal Malaysia Police

SA Robert Josh Williamson, Special Agent, FBI Legal Attaché Office Manila, Philippines
The first speaker, Mr Williamson, began his presentation by giving an overview of the Islamic State of Iraq and the Levant (ISIL), also known as the Islamic State of Iraq and Syria (ISIS) or the Islamic State of Iraq and ash-Sham. The Islamic State (IS) is a Wahhabi or Salafi jihadist state mainly composed of Sunni Arabs from Iraq and Syria who control territories there. It also has nominal control over small areas of Libya, Nigeria and Afghanistan. The group also operates or has affiliates in other parts of the world, including in North Africa and South Asia. The group was created in 1999 in Iraq by Abu Musa al-Zargawi.

Mr Williamson explained that the current financial status of ISIL was not reliant upon or integrated with the international financial system. In fact, most of the funding was derived internally and only a small portion of the total income originated from outside donors. He noted that Al Qaeda had a USD30 million income in 2014. However, ISIL is now making between USD1 to 5 million per day because its occupied territories have one of the largest oil fields and refineries in Iraq and Syria which produces an estimated 10,000-30,000 barrel per day.

Mr Williamson explained that another source of funding was oil revenue involving fuel smuggling. He noted that terrorists were using primitive methods in mini or mobile refineries and some fuel was transferred across the border on the Orontes River. Also he observed the other methods of funding were through criminal activities such as extortion, kidnapping for ransom, selling artefacts and antiquities, and theft.

He observed that other types of funding included taxation in the areas or territories controlled by ISIL. He emphasised that legal funding might come from donations from the Gulf States and humanitarian groups or non-governmental organisations (NGOs). Furthermore, terrorist funding might also come from individuals such as in the case of Mufid Elfgeeh, a Yemen-born man who managed a convenience store in upstate New York, United States.

Mr Williamson pointed out that to counter terrorist funding, financial institutions must monitor: NGO bank accounts; monetary instruments used in Syria or Iraq including debit cards; automated teller machines (ATMs); wire transfers involving Gulf States, Iraq and Syria and also banking activity in conflict areas. To counter ISIL funding activities, he suggested that financial institutions should be aware of terrorist financing trends, patterns and indicators. They could also initiate potential leads through identification of new individual clients and businesses. Finally, sanctions must be put in place to deal with apprehended terrorists.

Dr Muhammad Yusuf, Head, Indonesian Financial Transaction Reports and Analysis Centre (PPATK)
Dr Muhammad Yusuf began his presentation by explaining that the peaceful nature of Islam as emphasised in the Quran was to protect all human beings. He further elaborated that Indonesia’s action in countering terrorist financing had gained recognition from the Financial Action Task Force (FATF). He quoted the proverb from Carl Von Clausewitz, a Prussian general and military theorist, who stated that: “to achieve victory we must mass our forces at the hub of all power and movement. To conquer the enemies, we are required to find the centre of the power, the centre of gravity that belongs to the enemies. Thus, we can plan every capability we own, whether physical or non-physical strength, to counter the enemies’ requirements”.

Dr Muhammad explained that the centre of gravity in the context of terrorism lay in the financing of it. He explained that the attacks involving
the World Trade Centre in 2001 only cost USD450,000; and the train bomb attack in Madrid in 2004 only required USD10,000; the Istanbul truck bomb attack of November 2003 only cost USD40,000; the Bali bomb attack in 2002 cost USD50,000 and lastly the Mumbai attack in 2008 cost only USD10,000. The money involved in terrorist activities does not have to be considerable. With a small sum of money the damage to public property and even life can be severe.

He continued by explaining the Indonesian legal framework relating to the Anti-Money Laundering and Counter-Terrorist Financing Law No 9 of 2013 which deals with the Prevention and Eradication of Criminal Acts of Terrorist Financing. The other initiative is the joint regulation of persons and corporate identity and the Instant Blockage of Personal or Corporate Funds as Listed in The Alleged List of Terrorists and Terrorist Organisations. He emphasised that Indonesia had taken a major step in countering terrorist financing by amending the particular regulation to strengthen its counter-Terrorism efforts.

On the funding of terrorist groups he stated that the funds could be derived from various sources. Such sources included the proceeds of illegal activity, the proceeds from legitimate business activities, donations to charities and non-profit organisations, the commission of criminal activities and hacking of business websites. He stated that the uses of the funding were also varied ranging from military style training, the cost of living for members including food, accommodation and travel, purchasing materials for terrorist acts including firearms and weapons and acquiring false identification documents.
On the prevention of terrorist financing, Dr Muhammad observed that Indonesia’s current policy in preventing terrorist financing was by forming a joint task force consisting of the Head of PPATK, the Head of the High Court, the Head of the Indonesian Police, the Head of the BNPT, the Ministry of Foreign Affairs and KUHAP. Indonesia had also created a new contextual method for the interpretation of Al-Quran. He noted that the authorities had also organised training for the regulator (PPATK), the investigators, prosecutors, judges and lecturers.

Dr Muhammad believed that the Indonesian government had also enhanced the analytical capabilities of PPATK through building the capacity of PPATK employees from the global perspective. Supervision and regulation of non-profit organisations to monitor matters has been arranged and the Indonesian National Risk Assessment, especially with close reference to the risk of terrorist financing has been formulated and launched. Lastly, efforts have been made with regard to public education and awareness of how dangerous terrorism is, how to help prevent it and how to report it to the authorities.

Michael McGillion, Manager, National Security Operations, Australian Transaction Reports & Analysis Centre (AUSTRAC)

Mr McGillion began his presentation by explaining terrorist financing from the Australian perspective. He emphasised that terrorism is contrary to the precepts of Islam and that the Australian government is equally concerned with terrorist threats that do not employ the language of Islam. He then examined the seriousness of the terrorist financing threat to Australia. Not only do terrorist financing activities in Australia sometimes support terrorist groups overseas but terrorism financing can tarnish the credibility of Australia’s financial institutions.

He agreed with the previous speaker that the relatively small amounts of money required to fund terrorist activities could damage the reputation of Australian financial institutions. He explained that the collaboration between domestic agencies and partnerships with industry and the Australian community at large are important to combat terrorist financing. Mr McGillion mentioned that several Australians had travelled to Syria to engage illegally in terrorist groups associated with ISIS and that others had established relationships with the radical group in Syria.

Mr McGillion then explained the role of the Australian government in dealing with terrorist financing. He said that the government had taken steps to monitor compliance with the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 and took enforcement actions, where necessary, against violations of the Act.

Highlighting the impact of such financing, Mr McGillion suggested that financial support of terrorism presents systemic risks to Australia’s national security, economic system, commercial organisations and not-for-profit organisations (NPOs). However, he noted that terrorist funding was of primary concern as an enabler of terrorist acts both in Australia and overseas. He noted that in addition to funding individual terrorist attacks and operations, terrorism financing could help establish and maintain terrorist groups in Australia and other states and could also help maintain their communication networks.

Regarding the purposes of terrorist funding Mr McGillion agreed with the previous speaker in saying that it could be used to support the less violent aspects of terrorist operations such as paying for daily living expenses, travel, training, propaganda activities, organisational costs, and compensation for wounded fighters or the family members and dependents of terrorists who have died. He concluded his presentation by discussing financial methodologies associated with a terrorist travelling to participate in a foreign conflict. Possible sources of funds for foreign terrorist fighters include personal savings (including retirement savings accounts), application for credit from financial institutions, and selling of personal assets. The use of funds prior to departure can include purchasing airfares, mobile phones and clothing suitable for combat scenarios. Foreign terrorist fighters may seek to access funds while in-theatre through the use of stored value (prepaid) cards, internet banking and remittances made by family and close associates. Mr McGillion encouraged the reporting of STRs demonstrating these indicators as early as possible, as even partial or incomplete information may be able to complete the picture for security agencies and enable a response to the threat before the foreign terrorist fighter departs.

Q & A Session

The session ended with the moderator explaining that Malaysia might have relevant training in dealing with terrorists as the country had a long history dealing with communist groups. In response to a question from an audience member on the issue of the number of young Muslim foreign fighters in Australia, Mr Williamson responded by stating that their high motivation for terrorism derived from their misunderstanding of martyrdom and jihad and also because of their lack of understanding of the proper teachings of the Quran.
PLenary session 6: Financial Crime Investigations: An International Perspective

Speaker: Karyn Kenny
Resident Legal Advisor, U.S. Embassy Malaysia

Ms Kenny began by emphasising that the main objectives of her presentation were to give an insider’s view on the efforts of the U.S. Department of Justice to deal with global financial investigation cases. She divided her speech into four main parts. First, she gave a brief personal introduction and some background on the U.S. Department of Justice; next she dealt with global trends in transnational crime; third, she highlighted financial investigations which AML Compliance Officers should be aware of; and finally she identified three U.S. financial crime prosecution case studies.

Ms Kenny then discussed the role of the U.S. Department of Justice’s (DOJ) Office of Overseas Prosecutorial Development, Assistance & Training (OPDAT) Resident Legal Advisor to the U.S. Embassy in Malaysia. Previously she served as the International Attorney Advisor at the U.S. Department of Justice. In her early career as an Assistant District Attorney in New York City she prosecuted violent crimes. Later she served as an Assistant U.S. Attorney specialising in financial fraud cases. She was also a Supreme Court Fellow with the Supreme Court of the United States.

Speaking about the U.S. Department of Justice (DOJ), also known as the Justice Department, she explained that the DOJ is the federal executive department of the U.S. Government which is responsible for law enforcement and also the administration of justice in the United States. The DOJ is headed by the United States Attorney General who is nominated by the President, confirmed by the Senate and is a member of the Cabinet. The Office of the Attorney General was created by the Judiciary Act of 1789 and its mission is to enforce the law and defend the interests of the United States according to the law as well as to ensure fair and impartial administration of justice for all Americans.

She then proceeded to talk about transnational financial crime, which she stated was not stagnant, but ever-changing, adapting to markets and creating new forms of illicit income. In July 2011 President Obama signed the Transnational Criminal Organizations (TCO) which declared a national emergency on Transnational Organized Crime (TOC). This order re-conceptualised TOCs as national security threats and introduced successful tools in the fight against terrorism. She gave examples of TCO crimes as being money laundering, terrorist financing, banking fraud, tax fraud, mail or wire fraud, credit card fraud, embezzlement, blackmail, corruption, counterfeiting, insider trading, racketeering and organised crime smuggling.

In terms of financial investigations, Ms Kenny stated that these investigations were similar to other types of criminal investigations in approach and method. By using the same investigative skills a financial investigator would seek to trace the finances of criminals and discover how much they made from their criminal enterprises. This approach would serve to link any activities with the illegal proceeds of those activities. She explained that the financial investigation process involved identifying the relevant statute and finding evidence to prove the crime; tracing and documenting the transactions involved; preserving the evidence and finally presenting such evidence obtained by the prosecutors to the court.

Ms Kenny then gave an example of a drug trafficking case involving the suppliers, distributors, dealers, sellers and buyers. The drug supplier, through his drug trafficking organisation, ran the drug trade in the street. The drug supplier would give his narcotics associates or agents...
different responsibilities ranging from picking up and transporting the drugs for distribution, to running the daily operations and also collecting the proceeds from drug sales. The organisation will also employ street-level workers responsible for selling the drugs to buyers on the street.

The speaker then proceeded to deal with three main case studies: the Black Market Peso Exchange (BMPE), the Wire Stripping 101/U-Turn Payments involving Lloyds TSB Bank, and a drug money laundering scheme involving the Union Bank of California. In the BMPE case the drugs were smuggled into the U.S. and the drug traffickers had U.S. dollars in U.S. but needed to turn them into pesos in Colombia. Meanwhile the business owners in Colombia had pesos and needed to get U.S. dollars. The BMPE brokers bought dollars from the drug traffickers and sold them to the business owners. Every day in New York City workers for the drug
Financial institutions must continuously adopt procedures or safeguards to ensure compliance. They must also utilise the best available interdiction software to execute screening for wire transfers and new accounts.

Karyn Kenny

Lloyds agreed to a settlement of USD$217,000,000 and also agreed to provide financial information relating to the illegal transactions.

The last case study discussed by the speaker was the Union Bank of California involving violations of the Bank Secrecy Act. With this example, the drugs money laundering scheme involved Mexican exchange houses known as Casas de Cambio. The Union Bank failed to stop millions of dollars of suspected drug proceeds moving through accounts held at the bank by the exchange houses. Instead of directly depositing their U.S. drug profits, the drug networks increasingly moved money in bulk over the border, deposited them at the Mexican exchange houses, and then wired the dirty money to Colombia through the U.S. banks. The Union Bank failed to monitor the Mexican Casas de Cambio transactions and report any suspicious activity, despite being aware of the heightened risk of money laundering posed by those bank customers.

The speaker ended her speech by sharing some lessons that could be learned from these financial crime investigations. She emphasised that financial institutions must continuously adopt procedures or safeguards to ensure compliance. They must also utilise the best available interdiction software to execute screening for wire transfers and new accounts. Regarding human resources, financial institutions must train their employees to identify or respond to transactions with OFAC risks and they should employ experts who can understand the criminal movement of money.

Finally she suggested that the cooperation between the public and private sectors within this particular area was crucial.

Q & A Session
Ms Kenny responded to a question from the audience about the role of the grand jury in the United States. She explained that the grand jury played an essential role in the criminal process, but not one that involved finding guilt or determining punishment of the accused. Instead, a prosecutor will present evidence to the grand jury, who then decides whether or not to vote an indictment, also known as true bill, against the accused. Unlike trial juries, grand juries do not decide if someone is guilty of the criminal charges that have been brought against them. Grand juries listen to the evidence and decide if someone should be charged with a crime.

In both the state and federal systems, if the grand jury finds probable cause exists to support criminal charges against the accused person, the grand jury will vote a true bill. In other words, the grand jury, and not a judge or a prosecutor, makes the neutral determination whether or not there is in fact a factual basis for the criminal charges. The next major step, short of a plea deal or dismissal, is the trial. State grand juries sit for varying terms depending on the state; a grand jury may sit for a month, six months, or even a year.
Jeyashanker Kandasamy  
Senior Vice President, AmBank Group  
Compliance

The conference ended with closing remarks by Mr Kandasamy of the Compliance Officer Networking Group. He complimented the organisers, speakers, moderators, rapporteurs and sponsors for another successful and productive conference. Mr Kandasamy reiterated the point made in the keynote address on the timeliness of the theme of the conference. He observed that compliance officers were under tremendous pressure and that this pressure was due to the changing regulatory landscape facing financial institutions. Compliance officers have to strive to overcome the challenges involved in their jobs as financial markets are still growing.

Mr Kandasamy and the organisers believed that due to all these challenges the Conference theme was indeed timely. The speakers, the subject matter experts and the regulators had been invited specifically to share with the participants their insights and thoughts on the changing regulatory landscape. It was the hope of the organisers that the insights gained from the conference would be beneficial to compliance officers and enable them to deal more effectively with the new challenges.

Mr Kandasamy ended his closing remarks by quoting a speech by the late US President Theodore Roosevelt, who said: “Far better is it to dare mighty things, to win glorious triumphs, even though checkered by failure; than to remain with those poor spirits who neither enjoy much nor suffer much, because they live in a grey twilight that knows not victory nor defeat. We have too much to do. To sit on the side-lines, no. We need to step out of the grey twilight, to the bright sunshine so that we can see the dawn of a new day”. On that note, he bid all the delegates a safe trip home.
Conference Photo Gallery
Acknowledgements

Platinum & Merchandise Sponsor:

LexisNexis®

RISK SOLUTIONS

Gold Sponsor:

BAE SYSTEMS

INSPIRED WORK

Exhibitors:

DOW JONES

SWIFT

TESS INTERNATIONAL

THOMSON REUTERS

ACCELUS