2014

REGULATORY AND SUPERVISORY FRAMEWORK

The regulatory and supervisory framework continued to be strengthened in 2014, driven both by the global reform agenda as well as domestic priorities. A key focus of regulatory measures was on the implementation of the Basel III liquidity standards for the banking sector and the development of the regulatory framework for financial groups to support consolidated supervision by the Bank.

The Bank also completed reviews of a number of existing prudential standards relating to risk management as well as oversight and other control functions to further guide and elevate the standards of risk management practices in the financial sector. This included the finalisation of proposed changes to current standards on corporate governance to provide for more consistent approaches across all licensed financial institutions and to further strengthen the effectiveness of boards. The regulatory framework for development financial institutions (DFIs) is also being further strengthened to better support the specific mandates of these institutions in promoting more inclusive growth in a sustainable manner. To this end, the Bank, working closely with relevant Ministries, is in advanced stages of recommending amendments to the Development Financial Institutions Act 2002 (DFIA) which are expected to be tabled to Parliament in the first half of 2015.

The implementation of the Basel III liquidity standards and development of the regulatory framework for financial groups were key focus areas in 2014

In November 2014, the Financial Action Task Force (FATF) and the Asia Pacific Group on Money Laundering (APG) concluded an on-site assessment of Malaysia's compliance with the International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation. The assessors observed well-developed institutional arrangements for the supervision of anti-money laundering and countering the financing of terrorism (AML/CFT) risks in the banking and insurance sectors.

STRENGTHENING THE PRUDENTIAL FRAMEWORK

Regulation of financial groups

The Financial Services Act 2013 (FSA) and Islamic Financial Services Act 2013 (IFSA) introduce provisions for the supervision of financial groups to ensure that material risks from group-wide activities are effectively managed and controlled. Under the new laws, financial holding companies (FHCs), defined as apex entities of financial groups which are not licensed persons, are required to be approved by the Bank. FHCs are also required to observe relevant group-level prudential standards. The Bank has identified 16 companies that qualify as FHCs. As at end-January 2015, ten companies have been approved as FHCs, including eight which were identified prior to the enactment of the FSA and IFSA. The remaining six have submitted applications and are expected to be approved by the end of 2015. A key consideration in approving an FHC is whether oversight at that level would provide the Bank with an adequate view of material group-wide risks which may affect licensed institutions within the group. The Bank also considers the extent to which reliance can be placed on consolidated supervision performed by a competent home regulator in the context of foreign-owned financial groups. Where this reliance can be established, supervision on a solo basis of licensed institutions in Malaysia that are within the group is sufficient.

Ten companies have been approved as FHCs as at end-January 2015 and six other companies are expected to be approved by the end of 2015

The first set of prudential standards being developed is the capital framework for banking groups. Following the implementation of higher capital standards for banking institutions under

the Basel III reforms in 2013, the Bank issued a discussion paper in October 2014 setting out its intention to extend the existing capital adequacy framework for banking institutions to banking groups headed by FHCs. An FHC of a banking group will be required to measure, monitor and comply with capital requirements on a consolidated basis at the group level. The objective is to ensure that there is sufficient capital to support risks originating from both regulated financial institutions and unregulated entities within a group. It also aims to reduce leverage associated with the multiple gearing of capital which can overstate a group's capital strength and increase contagion risk within the group. In addition, the implementation of group-wide capital standards will enhance the comparability between disclosed capital ratios for banking groups headed by FHCs and those headed by licensed banks. This, in turn, will further improve conditions for effective market discipline.

The Bank had received feedback to review the condition for capital instruments issued by banking subsidiaries to contain group-level loss absorbency triggers. Currently, qualifying capital instruments issued may be converted into equity or written-off in certain trigger events, namely when capital falls below predetermined levels, or where the bank is declared to be non-viable. With the inclusion of a group-level loss absorbency trigger, such capital instruments may also be converted or written-off if these triggers are met at the financial group level. The Bank will further examine these issues as more progress is made in the implementation of recovery and resolution plans (including in a cross-border context) for financial groups. The Bank will also undertake further work on: (i) the future impact of including a group-level trigger on the ability of banks to raise affordable loss-absorption funding; and (ii) the role of a group-level trigger in amplifying group contagion risk caused by non-regulated affiliates. The Bank expects to issue the final standards in 2015, while compliance with the minimum group capital requirements are expected to take effect from 1 January 2019.

Liquidity standards

Work to strengthen liquidity standards as part of the implementation of the Basel III reform package was completed during the year. Following a two-month consultation period, the Bank will publish the final Liquidity Coverage Ratio (LCR) standards in March 2015. The new rules will take effect from 1 June 2015 and will be phased in according to the global implementation timeline illustrated in Table 3.1.

The new standards will replace the existing Liquidity Framework (LF) which has been in place since 2000. Similar to the LF, the LCR requires a banking institution to maintain adequate liquidity buffers to sustain itself through a 30-day liquidity shock. However, the LCR improves on the cash flow assumptions by reflecting the possibility of more severe liquidity shock scenarios, such as that experienced during the past global financial crisis. While largely consistent with the Basel III rules, the LCR standards have taken into account the structural and behavioural characteristics of the financial system in Malaysia, as well as industry feedback. This is particularly relevant for the classification of high-quality liquid assets (HQLA). Under the Basel rules, there are three tiers of HQLA, namely Level 1, Level 2A and Level 2B assets – with Level 1 assets being of the highest quality. In determining the scope of HQLA under the LCR standards, the Bank has considered the size and depth of the market for eligible instruments as well as the liquidity of these assets. Based on an analysis of these factors, the Bank has adopted a more conservative treatment for the recognition of `AA'-rated and `A'-rated corporate bonds as HQLA. In the case of the latter, recognition is confined to non-ringgit corporate bonds which are internationally rated. This is counterbalanced by lower haircuts applied in limited circumstances to specific categories of HQLA such as high-quality residential mortgage-backed securities issued by Cagamas MBS Berhad.

The LCR standards also define the treatment of Islamic investment accounts. Consistent with the overall design of the LCR framework, investment

Table 3.1

LCR Implementation Timeline

Year	1 June 2015	1 January 2016	1 January 2017	1 January 2018	1 January 2019 and thereafter
Minimum LCR requirement	60%	70%	80%	90%	100%

account funds are assigned run-off rates based on the relative stability of the funds. Indicators of stability include the existence of contractual features (such as redemption conditions), liquidity features of underlying assets and the type of investment account holder. The approach adopted in the LCR standards reflects the liquidity treatment of investment accounts proposed by the Islamic Financial Services Board in October 2014.

The Bank also confirmed several other measures including the recognition of statutory reserves as Level 1 assets and the eligibility criteria for term deposits to be excluded from a bank's LCR calculation.

Based on earlier observation data, banking institutions are expected to be able to meet the first interim minimum LCR level of 60% with relative ease. 30 out of 54 banking institutions are already reporting LCR levels above 100%. The Bank continues to closely monitor the impact of the LCR standards on financial markets and credit conditions, particularly in the present environment of increased volatility in the financial markets and greater competition for deposits from alternative savings and investment avenues. The Bank has intensified its supervision of banking institutions that will need to take more substantive measures to prepare for full LCR compliance in 2019. The Bank will analyse the cumulative impact of measures taken by individual institutions with the aim of identifying and mitigating any unintended consequences.

The new LCR standards will take effect from 1 June 2015 and will be phased in over four years

Corporate governance

Enhancing corporate governance and risk management practices continued to be a key focus for the Bank in 2014. During the year, the Bank concluded a broad review of the corporate governance framework for financial institutions. While financial institutions have made significant strides in enhancing corporate governance practices in recent years, it is important for industry practices to continue to evolve to account for operations that have become inherently more complex. Market innovations, cross-border expansions and increasing financial conglomeration are the main drivers of this complexity. Drawing on supervisory observations, engagements with the industry and lessons from the global financial crisis, the review identified a number of areas which would benefit from additional clarity and strengthened requirements to help boards function more effectively. The Bank expects to publish a concept paper in the first half of 2015 which will set out its proposals to enhance the quality of corporate governance practices in the banking and insurance sectors.

The concept paper will introduce a more comprehensive definition of independent directors and the requirement for higher representation of such directors on the boards of financial institutions. The paper will also clarify the Bank's position on the involvement of group executives on the board of a financial institution. Where group management responsibilities are likely to impinge on the ability of group executives to objectively oversee management actions (for example due to their direct involvement in taking management decisions that affect the financial institution), a group executive will be subjected to the maximum limit imposed on the number of executive directors that can be represented on the board. The Bank is also seeking further feedback on approaches to enforcing term limits for independent directors.

The revised standards will also be applied to FHCs that are approved by the Bank. An FHC will be required to comply with the same standards for its own board and management which are responsible for ensuring effective oversight and control of the financial group. The proposals further clarify the Bank's expectations in situations where financial institutions seek to leverage on centralised governance structures established by the FHC. These requirements aim to preserve a clear focus on the sound management of individual licensed institutions within the group, while encouraging a consolidated view of risks throughout financial groups and across the jurisdictions where they operate.

Risk management and internal controls

To complement the overarching risk governance standards issued in 2013, the Bank has worked to put in place a set of expectations on key controls and cultural norms in significant risk areas that can expose financial institutions to financial losses or reputational damage. In September 2014, the Bank consulted with the industry on proposals to elevate the standards of compliance practices in the financial sector. This comes at a time when

the financial industry is facing a more challenging regulatory environment. In addition to prudential and market conduct standards that are evolving in response to emerging risks, the implementation of new competition, data protection and tax legislation has also substantially increased the compliance obligations of financial institutions.

The proposed compliance standard addresses the need for financial institutions to establish an effective compliance programme to monitor and ensure that institutions are meeting their obligations under applicable laws and regulations. The Bank expects such a programme to reflect the primary responsibility of business lines for managing compliance risk emanating from business operations. Financial institutions will additionally be required to set up a compliance function, led by a chief compliance officer, that would be responsible for keeping the board and senior management regularly informed on the overall state of compliance and significant compliance issues affecting the institution. An important objective of the compliance standard is to ensure that the board of financial institutions are giving the compliance function sufficient authority, resources and oversight for them to function effectively and to avoid costly compliance failures. The Bank expects to issue the final standard in the first half of 2015.

The compliance function must be given sufficient authority, resources and oversight appropriate for it to function effectively

The Bank also worked towards finalising the standard on operational risk management. Concerns over operational risks have increased over the past decade as financial institutions have grown larger, more dependent on technology and more interconnected with the broader financial system through a variety of channels, including shared services and market infrastructure. The standard requires financial institutions to have more robust and systematic processes in place for identifying, assessing and controlling the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events. Financial institutions should demonstrate that controls over operational risks are commensurate with the institution's size and level of operations. In this respect, active financial market players and large financial institutions are required to establish an operational risk control function and a dedicated sub-committee within each significant business and functional line. This acknowledges the considerable diversity in the nature of operational risks which can be easily overlooked in large and complex businesses. The Bank expects to issue the final standard in the first half of 2015.

The Bank also launched ORION, an operational risk surveillance system, to support the implementation of the standards. Financial institutions are required to report events that result in financial losses, any operational risk incidences and outcomes of scenario analyses based on potential operational risk catastrophes. The collection of high quality data over time will support better analysis of operational risk trends in the industry.

Outsourcing

The drive to improve operational efficiency and gain greater flexibility to manage business change has resulted in more extensive outsourcing by financial institutions in recent years. Financial institutions are increasingly outsourcing a broader range of internal processes and functions to affiliates and third-parties in Malaysia and abroad as they seek to strengthen their focus on core business activities and leverage on group synergies and other opportunities to tap into the best services and technology available.

However, if not effectively managed, outsourcing arrangements can increase risks to financial institutions. These include risks associated with the loss or abuse of customer data and delays or gaps in access to information that can impede an institution's ability to monitor and control its risk exposures. A key concern of the Bank is also its ability to verify that financial institutions are meeting their regulatory obligations in respect of functions performed by third-parties. Over-dependence on other parties, especially within the context of financial groups where complex webs of interdependencies exist, may hamper efforts

to recover critical business functions or resolve financial institutions in an orderly manner.

Given the more extensive nature of outsourcing observed within the financial sector, the Bank decided to review existing prudential frameworks on outsourcing activities for financial institutions. The Bank will issue a concept paper in the second half of 2015 that updates and consolidates existing sector-specific requirements into a single set of enhanced standards. Important enhancements in the proposed outsourcing standards include: (i) subjecting specific outsourcing arrangements which relate to an institution's significant business activities to supervisory approval; (ii) improved processes that must be in place for identifying critical business functions and for which enhanced due diligence must be performed on prospective service providers; and (iii) a requirement for financial institutions to develop and test contingency plans to prepare for the sudden termination of an outsourcing arrangement. While the Bank acknowledges the benefits of outsourcing through group synergies, the standards will state the boundaries within which outsourcing arrangements should operate. This is to ensure that individual licensed institutions in Malaysia remain fully accountable for complying with local regulations. Moving forward, all outsourcing agreements must also include provisions that guarantee the continuity of services in the event of resolution of the financial institution concerned. Agreements must additionally clarify the Bank's ability to access any information held by the service provider which is relevant to the outsourced activity.

Standards are being enhanced to ensure that the ability of financial institutions to effectively monitor and control risk arising from outsourcing arrangements is not compromised

Limit on exposures to single counterparties
The limit on exposures to single counterparties (SCEL) is a key component of the prudential framework. The objective is to protect banking institutions from large losses resulting from the sudden default of a single counterparty. In July 2014, the SCEL was revised to allow banking institutions to maintain exposures of up to 50% of total capital (instead of 25%) to related banking entities with the Bank's prior approval. As is common in many jurisdictions, the treatment provides greater flexibility for accommodating short-term intra-group exposures which may arise in the delivery of financial products and services as part of group operating models. In approving the higher limit, the Bank will consider whether: (i) there are legal or practical restrictions which may prevent a related banking entity from transferring capital resources or repaying liabilities to the banking institution; (ii) the related banking entity is subject to adequate prudential regulation and supervision in its jurisdiction and complies with an equivalent SCEL framework on a consolidated basis; and (iii) the Bank will have timely access to relevant information on the related banking entity for supervisory purposes.

Following the Basel Committee's finalisation of the supervisory framework for measuring and controlling large exposures in April 2014, the Bank may consider further adjustments to the SCEL framework after a more detailed examination of the global standard and its implications if applied within the context of the Malaysian banking system.

Regulatory framework for Islamic finance
During the year, the Bank made further progress in the development of a Shariah contract-based regulatory framework.

To date, the Bank's Shariah Advisory Council (SAC) has approved the Shariah parameters for eight contracts, namely *murabahah, mudarabah, musharakah, wadi'ah, bai'inah, ijarah, tawarruq* and *hibah*. The Shariah parameters for four other contracts, namely *istisna', wakalah, kafalah* and *wa'd* will be reviewed by the SAC in early-2015. Following this, the Bank will issue operational standards to ensure that products structured using such contracts comply with sound governance, risk management, documentation, disclosure and market conduct requirements. The Bank issued the final operational standards for *murabahah* in 2014, and expects to finalise the operational standards for *musharakah*, *mudarabah*, *ijarah* and *istisna'* in the first half of 2015. Industry consultations for standards relating to *tawarruq, wadi'ah, hibah, bai'inah, kafalah, wakalah* and *wa'd* will take place in 2015.

The implementation of these operational standards will broaden the range of Islamic finance products offered, enhance transparency and consistency

in the application of Shariah contracts in Islamic financial transactions, and ensure end-to-end compliance with Shariah principles.

In March 2014, the Bank issued the final standards to promote the sound management of Islamic investment accounts. Unlike deposits, Islamic financial institutions do not guarantee the repayment of principal on Islamic investment accounts. However, Islamic financial institutions still have the responsibility to exercise sound oversight over the management of these investments and ensure compliance with Shariah principles. Islamic financial institutions are also required to put in place adequate risk management arrangements to ensure fiduciary duties are discharged in accordance with the investment mandate agreed with the investors. The standards also specify minimum requirements on fair dealings for the protection of investors, as well as disclosure requirements to help investors assess the characteristics and performance of their investments. Islamic financial institutions have begun migrating existing customer accounts to either deposit or investment accounts as required by the IFSA, and this is expected to be completed by June 2015. As part of this process, customers will be provided with information on alternative IFSA-compliant deposit products that they can continue to maintain their funds in, or an option to participate in investment accounts.

The implementation of operational standards for Shariah contract-based products enhances consistency in the application of Shariah contracts in Islamic financial transactions and ensures end-to-end compliance with Shariah principles

Prudential framework for insurers and takaful operators

A key prudential requirement for insurers and takaful operators is the preparation of the financial condition report (FCR) by an appointed actuary. The FCR serves to provide the board with critical insights on changes in the operating environment and risk profile of the insurer or takaful operator. The report also serves as a valuable source of independent advice to the board on options available to mitigate identified threats to the financial condition of an insurer or takaful operator. The requirement to prepare the FCR was introduced to life insurers in 2006 and was extended to general insurers in April 2014. The Bank issued a concept paper in December 2014 with proposals to improve the timeliness of the report, and to replace prescriptive rules with a more principle-based approach for the conduct of dynamic solvency testing by the appointed actuary. These enhancements aim to enable insurers and takaful operators to be more responsive to conditions affecting their business and for such conditions to be reflected in the stress testing parameters and scenarios used to perform solvency tests.

Participating policies form an important class of business in the life insurance sector in Malaysia. These policies provide policy owners with the opportunity to participate in the profits of the insurance fund, usually by way of bonus distributions determined by the insurer. The business has grown significantly over the years, accounting for 64% of total premiums collected by life insurers between January and September 2014. Given the significant discretion of insurers in determining bonus distributions and considerable diversity in insurers' practices in exercising this discretion, the Bank considered it important to address expectations surrounding the management of participating life business to safeguard the interests of policy owners. This resulted in a review of the standards on the management of participating life policies and the subsequent issuance of a concept paper in November 2014.

The Bank's proposals stipulate that the appointed actuary's recommendations to the board on bonus distributions must be supported by an appropriate bonus supportability study. Appointed actuaries must also consider the expectations of policy owners and assess the life insurer's compliance with regulatory requirements for the management of insurance funds. An insurer must have regard to the equitable treatment of policy owners in grouping policies together for the purpose of performing bonus supportability studies and in the management of the fund's estate. The concept paper also proposes to improve disclosures in sales and marketing literature and annual policy statements. This is to ensure that policy owners are not led to form unreasonable expectations on the payment of non-guaranteed benefits. The Bank is currently

reviewing the feedback received from the industry and expects to issue the final standards by mid-2015.

Enhancements to the financial condition report aim to enable insurers and takaful operators to be more responsive to conditions affecting their business

Amendments to the DFIA

Since its enactment in 2002, the DFIA has provided the foundation for a comprehensive regulatory and supervisory framework for DFIs. This has ensured that development mandates entrusted to DFIs by the Government are achieved in a financially sustainable manner.

In light of the changes to the financial services legislation, the Bank embarked on a review of the DFIA which led to the publication of a draft amendment bill for consultation in October 2014. The draft bill focuses on reforms in five areas, namely: (i) enhancing governance and risk management practices in DFIs; (ii) strengthening the mandates of each DFI in serving targeted segments in the Malaysian economy; (iii) promoting greater operational efficiencies; (iv) upholding compliance with Shariah principles; and (v) strengthening provisions for effective enforcement and supervisory intervention. The proposed amendments draw on key features of the FSA and the IFSA and aim to further strengthen the capacity of and confidence in DFIs in promoting inclusive growth. The amendments are expected to be tabled to Parliament in the first half of 2015.

SAFEGUARDING THE INTEGRITY OF THE FINANCIAL SYSTEM

AML/CFT framework

An effective AML/CFT regime protects the integrity of the financial system by preventing criminal elements from benefiting from the proceeds of illegal activities. Besides contributing to the national aspiration of reducing crime as outlined in the Government Transformation Programme, it also promotes domestic and international confidence in financial institutions that operate in Malaysia. As the Competent Authority under the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLA) and the Chair of the National Coordination Committee to Counter Money Laundering (NCC), the Bank plays a pivotal role in coordinating nationwide efforts to strengthen the AML/CFT regime in Malaysia. The NCC completed several key initiatives in 2014. These include amending the AMLA, developing the National Risk Assessment (NRA) and formulating a National AML/CFT Strategic Plan. These initiatives ensure that appropriate measures are taken at the national level to address areas that pose significant money laundering and terrorism financing (ML/TF) risks, and that these measures are supported by the effective implementation of a strong legal and regulatory framework.

Over the years, the Government has put in place a comprehensive legal and regulatory framework to combat financial crimes. In 2014, the AMLA was amended to strengthen regulatory requirements, further clarify obligations of reporting institutions and expand the powers of law enforcement agencies. The penalties upon conviction of an offence were substantially increased – a money laundering offence now carries a penalty of up to 15 years of imprisonment and a fine of not less than five times the value of the proceeds of the crime or RM5 million, whichever is higher. The scope of serious offences has also been expanded to include offences specified under other legislation such as the Wildlife Conservation Act 2010, Common Gaming Houses Act 1953, Penal Code and Immigration Act 1959/63. The expansion was a result of the NCC's ongoing assessment of the comprehensiveness of serious offences listed under the Act in response to emerging ML/TF threats in Malaysia. The amended AMLA came into force on 1 September 2014.

In June 2014, the NCC also completed the NRA, a process which began in 2012 to identify key vulnerabilities and ML/TF threats across various sectors in the country. The findings of the NRA have been vital in developing AML/CFT strategies and will guide the allocation of resources, skills and expertise necessary to address identified risks. NCC members and reporting institutions were informed of the key results of the NRA through a series of briefings.

The NRA identified five types of crime that pose the highest threat of money laundering and four sectors that are highly vulnerable to ML/TF

risks (Table 3.2 and Table 3.3). The NRA will be reviewed regularly to ensure it remains reflective of the prevailing ML/TF risk landscape. A review of the threat level for terrorism financing will be undertaken in 2015 to take into account the conclusions of the `White Paper on Terrorism Threats from the Islamic State Group' published by the Government in November 2014.

Based on the NRA results, a National AML/CFT Strategic Plan was developed by the NCC to address the identified threats and vulnerabilities

Table 3.2

Money Laundering Threat Level of Different Crimes

Type of crime	Threat level
Fraud	High
Drugs trafficking	
Corruption and bribery	
Smuggling offences	
Tax crimes	
Terrorism financing	Medium
Organised crimes	
Human trafficking and migrant smuggling	
Forgery	
Theft and robbery	
Counterfeiting of currency	

Type of crime	Threat level
Sexual exploitation	Low
Arms trafficking	
Counterfeiting and piracy of products	
Insider trading and market manipulation	
Murder	
Environmental crimes	
Extortion	
Kidnapping	
Sea piracy	

Table 3.3

Inherent Vulnerability of Different Business Sectors to Money Laundering Risks

Financial sectors	Vulnerability level
Banking (including BSN, Bank Rakyat and Agro Bank)	High
Money changing	
Non-bank remittance services	
Fund management and unit trust	Medium
Offshore banking	
Non-bank deposit taking	
Stockbroking	Low
Life insurance	
Money lending	
Non-bank cards	
E-money	
Development financial institutions (SME Bank, Bank Pembangunan and EXIM Bank only)	

Non-financial sectors	Vulnerability level
Casino	High
Lawyers	Medium
Offshore trust	
Company secretaries	
Real estate agents	
Onshore trust	
Gaming	Low
Jewellers	
Accountants	
Pawn broking	
Notaries	

at the national level. The key thrusts of the plan include promoting greater understanding of ML/TF risks and enhancing the investigation capabilities of enforcement personnel. The plan also includes efforts to intensify domestic and international co-operation and ensure compliance with regulatory and supervisory requirements through effective enforcement. In November 2014, the country underwent a Mutual Evaluation (ME) exercise conducted against the International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation by the FATF and the APG. Recommendations and gaps identified during the ME exercise will be incorporated in the strategic plan to further strengthen the country's efforts in combating ML/TF risks.

A National AML/CFT Strategic Plan was developed to address key threats and vulnerabilities at the national level

On the international front, Malaysia was accorded Observer status by the FATF in 2014. This is a step towards full membership, pending the outcome of the ME exercise which will be known in 2015. Membership of the FATF will not only demonstrate a strong commitment to combating money laundering and financing of terrorism, but also reflect a safe business environment in Malaysia and provide an important platform to advance initiatives on financial integration and Islamic finance.

Monitoring AML/CFT compliance by reporting entities

In 2014, the Bank carried out on-site examinations to evaluate the effectiveness of AML/CFT practices of reporting entities. These examinations were conducted on 85 financial institutions, 212 money services business licensees and 15 designated non-financial businesses and professions (DNFBPs) which included, among others, a casino and trust companies. The examinations on DNFBPs operating in Labuan were jointly conducted with the Labuan Financial Services Authority. These examinations focused on the effectiveness of customer due diligence (CDD) assessments, the comprehensiveness of suspicious transaction reports submitted to the Bank, and the robustness and adequacy of risk management controls. Supervisors observed greater understanding of ML/TF risks and the relevant AML/CFT obligations. However, several entities faced challenges in fully meeting CDD requirements. These challenges include the implementation of beneficial ownership requirements as well as the identification of domestic politically exposed persons and their family members and close associates. Further efforts will also be required to address the risks associated with terrorism and proliferation financing, such as by developing more effective ``red flags´´ to identify such transactions. Moving forward, the Bank will continue to intensify engagements with financial institutions and DNFBPs. These engagements aim to enhance the level of awareness and facilitate the exchange of information on the latest ML/TF trends and observations.

In view of the large number of DNFBPs (26,569 entities as at end-2014), the Bank issues self-assessment questionnaires (SAQs) to facilitate the supervision of AML/CFT risks in selected sectors. This approach enables the Bank to conduct more intensive supervisory engagements in areas that pose higher risk and with sectors that warrant greater attention. SAQs were first issued to law firms in 2011. Moving forward, the Bank intends to extend the SAQs to real estate agents, company secretaries and trust companies beginning from 2015. This will provide a more comprehensive assessment of the level of AML/CFT compliance across various sectors as well as a broader spectrum of views from different respondents.

Strengthening the money services business industry

The money services business industry (which comprises the money changing, remittance services and wholesale currency businesses) represents an important area of focus in the Bank's efforts to reduce vulnerabilities to money laundering risks. During the year, money services business transactions conducted through formal channels continued to grow. Outward remittances amounted to RM32.1 billion, representing an increase of 27.8% over the RM25.1 billion registered in 2013. This growth was contributed by greater public awareness on the importance of using legal channels for remittances, along with wider provision of mobile and internet remittance services. Non-bank remittance service providers also continued to provide a convenient and cost-efficient alternative to banks for small businesses to make trade payments. This alternative added to the increasing use of formal

channels for remittances. In the money changing sector, domestic wholesale currency businesses transactions increased substantially by 40.8% to RM6.6 billion. This has been supported by the increase in wholesale currency distribution channels, particularly in areas where transactions of money changing are high and active. In the retail segment, the money changing business turnover experienced a marginal drop of 0.7% to RM52 billion due to lower demand for certain foreign currencies such as Chinese renminbi during the year. All licensed money changers have implemented computerised systems that are able to capture and consolidate details of money changing transactions. The implementation of computerised systems will facilitate ongoing monitoring of suspicious transactions.

Twelve money services business licences were not renewed by the Bank during the year due to significant non-compliances with regulatory requirements. A further 24 licensees voluntarily surrendered their licences as a result of mergers or conversion to agents for larger principal licensees. This reduced the number of licensees in the industry to 426 as at end-2014. Notwithstanding the reduction in the number of licensees, the provision of money services to the public remained widely distributed across the country. This is due to the expansion of branch and agent networks by larger and more established licensed money service providers. The expansion has also allowed smaller players to remain in the industry, while being able to leverage on the systems and controls of larger principal licensees in areas such as record keeping and AML/CFT compliance.

Outward remittance transactions conducted through formal channels continued to grow, increasing further by 27.8%

Progress continues to be made towards improving the effectiveness of AML/CFT policies and practices across the industry. With the enhanced policies on AML/CFT in place, greater consistency in the conduct of CDD and improvements in the identification of high risk transactions by licensees were observed. These developments pave the way for the adoption of a risk-based approach to identifying, assessing and mitigating ML/TF risks which was introduced to the industry in January 2015. During the year, the Bank also intensified its supervisory engagements to ensure that the IT systems of money services providers are sufficiently robust to support the documentation requirements under a risk-based approach.

The Malaysian Association of Money Services Business (MAMSB) continues to play an important role in supporting improvements in the industry's implementation of effective AML/CFT programmes. This included the organisation of a series of intensive and practical structured training programmes to educate members of the industry on compliance with AML/CFT requirements and reference manuals and procedures. During the year, the association, in partnership with the Bank and the World Bank, organised the Regional Conference on Money Services Business, attended by participants from 28 countries, to share international perspectives on developments, trends and challenges in the money services business industry. The association also worked closely with system providers to ensure that solutions provided are adequately designed to help licensees meet their compliance obligations. Typologies are also being developed together with the Bank to educate and assist the industry in understanding and identifying potential ML/TF risks arising from money services business. The association also plays an important role in spearheading initiatives to elevate standards of compliance and professionalism in the industry. During the year, the association drew up a code of conduct to instil market discipline and guide the industry for professional and ethical business conduct.

ENFORCEMENT ACTIVITIES

Strengthening the enforcement framework

The Bank is given broad enforcement powers under the laws that it administers to safeguard the stability and integrity of the financial system. A robust governance process ensures that any enforcement action undertaken by the Bank is justified, and that a due process is consistently applied across various sectors and institutions in similar circumstances.

In light of the expanded enforcement powers accorded to the Bank by recently enacted legislation (including the power to impose administrative and monetary penalties, issue public reprimands and pursue civil actions), the Bank further strengthened its existing enforcement procedures under a new framework which was adopted in

January 2014. This framework is governed by an Enforcement Committee (EC), which is the apex decision-making authority within the Bank on enforcement matters. The EC is chaired by the Governor and its members include the Deputy Governors and Assistant Governors responsible for regulation, supervision, legal and enforcement. The EC decides on enforcement actions to be taken in individual cases for breaches of the law and regulatory requirements. Any enforcement action by the Bank will be guided by a set of factors which include the effectiveness of the enforcement action, the proportionality of the action to the committed offence and whether such action results in the deterrence of future breaches of a similar nature.

The enforcement framework also sets out how the Bank will determine the amount of monetary penalties imposed for breaches of the law. This is to ensure that a consistent process is followed for offences of a similar nature. As required by the FSA and IFSA, the Bank established the Monetary Penalty Review Committee (MPRC) whose members are independent of the Bank's executives. The MPRC considers appeals relating to the quantum of administrative monetary penalties and pecuniary remedies enforced by the Bank. Under the law, a person aggrieved by the Bank's decision may file an appeal to the MPRC within 21 days after being notified of the Bank's decision. Further information about the MPRC, including its membership and the appeal process can be found on the Bank's website.

The Bank further strengthened its existing enforcement procedures under a new enforcement framework which was adopted in January 2014

Enforcement activities in 2014

Effective and timely enforcement action ensures that financial institutions are operating in compliance with applicable laws and regulatory requirements and consumers are protected from unauthorised activities that could result in financial losses to consumers. During the year, a total of 1,104 charges brought by the Bank were convicted by the court. The Bank also initiated 42 investigations and pursued 119 criminal charges against entities and individuals operating illegal schemes and activities. In addition, 536 offences were identified against licensees for non-compliance with laws and regulatory requirements. Table 3.4 contains a summary of the enforcement actions taken in 2014.

Table 3.4

Enforcement Actions Taken in 2014

Illegal deposit taking	• Nine charges pursued under the Banking and Financial Institutions Act 1989 (BAFIA) against two entities and six individuals for illegal deposit taking offences. • 11 charges were convicted under the BAFIA against four entities and eight individuals.
Money laundering	• One civil forfeiture under S56(1) of AMLA involving RM129,275. • 68 charges pursued under S4(1) of AMLA against one individual. • 1,083 charges convicted under the AMLA against seven individuals.
Unauthorised provision of money services	• 27 charges pursued under the Money Services Business Act 2011 (MSBA) against 26 entities and individuals for unauthorised provision of money changing services. • 15 charges pursued under the MSBA against one entity and seven individuals for unauthorised provision of money remittance services. • 10 charges convicted under the MSBA against seven entities and individuals for unauthorised provision of money services business.
Non-compliance with AML/CFT policies under AMLA and FSA	• Compound amounting to RM4.37 million against 11 banking institutions. • Compound amounting to RM62,000 against two money changing institutions.
Contravention of foreign exchange administration rules	• Compound of RM800,000 against one banking institution for contravention of S214(2) of the FSA. • Compound of RM80,000 against one money changing institution for 40 non-compliances under the Exchange Control Act 1953.

Management of Cyber Risks

Technology has played a transformative role in the provision of financial and payment services. In addition to improving the efficiency of processes, technology has opened up new and innovative channels for financial institutions to provide greater access and convenience to consumers. Technology has also enabled financial institutions to viably offer and manage a wider range of products that are competitive and responsive to different needs of consumers in ways that were not possible before. Business and retail customers have readily embraced these technological developments, as evidenced by the value of commerce transacted online which continues to rise.

These advancements however present new challenges for risk management by financial institutions. With increasing dependence on technology, financial institutions face new risks of malicious actions by criminals and other malefactors. These actions have the potential to disrupt the provision of services and also undermine the confidentiality and integrity of a financial institution's proprietary and customer data. Such incidents can thus damage the reputation of a financial institution and may undermine confidence in the financial system.

Global economic losses resulting from cybercrimes were estimated to be approximately USD375 billion annually[1]. Cyber attacks are commonly motivated by financial gain but can also be driven by an aim to cause disruption for social and political purposes. Following several high-profile cyber security incidents in the financial sector, the management of cyber risks has become an increasing global concern. A report[2] by the Committee on Payments and Market Infrastructure of the Bank for International Settlements emphasised the complex and rapidly evolving nature of cyber risks, and highlighted the increasing priority accorded to the effective management of these risks. The report also recommended a more integrated approach to cyber resilience, which will reduce recovery times in the event of a successful cyber attack, whilst enabling key functions of critical systems to continue to operate. In the European Union, the Joint Committee of the European Supervisory Authorities has similarly called for authorities and financial market participants to ensure that sufficient resources and attention are devoted to increasing the financial system's resilience against IT-related operational and cyber risks.

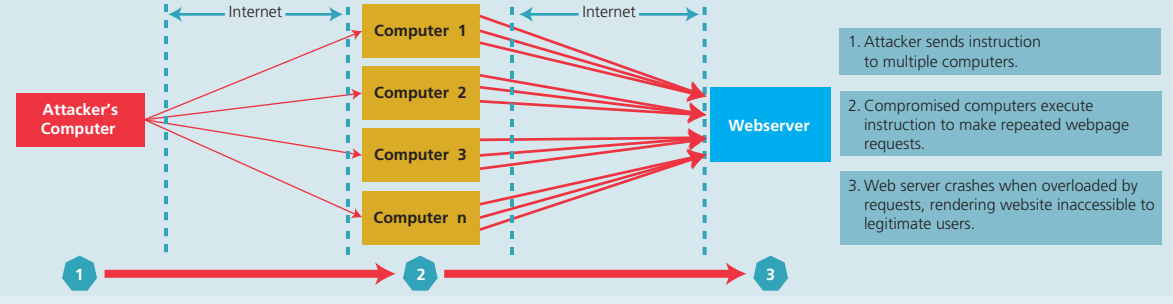
Forms of Cyber Threats

Cyber attacks against financial institutions are becoming more sophisticated and can take many forms. There are three common threats in the financial sector:

Distributed Denial of Service (DDoS) – In a DDoS attack, a targeted system is disrupted by directing a large flow of traffic to overwhelm it, thereby denying access by legitimate users. A network of compromised computers is directed to simultaneously make repeated requests (such as a particular web page) from the system (Diagram 1). Experts estimate that the number of DDoS attacks worldwide

Diagram 1

Distributed Denial of Service (DDoS) Attack on a Website



Source: Bank Negara Malaysia

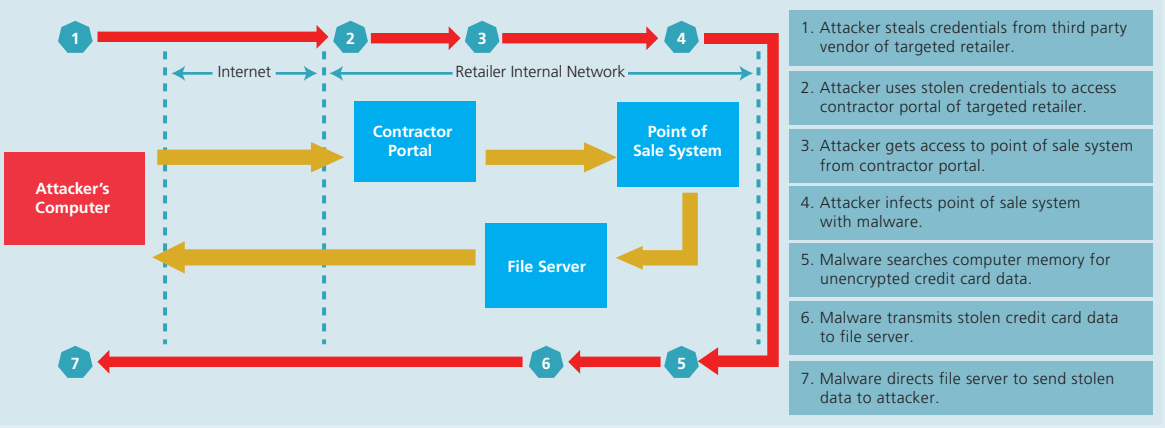
[1] Source: `Net losses: Estimating the global cost of cybercrime´, a report by the Center for Strategic and International Studies.
[2] Source: `Cyber resilience in financial market infrastructures´, November 2014.

have increased by 20% over the last two years, averaging almost 3,000 incidents per day, of which 43% were targeted at financial service providers[3]. DDoS attacks have been launched to disrupt customer access to the Internet banking portals of a number of global banks for hours or even days at a time, preventing customers from conducting online transactions. While DDoS attacks were experienced by some banks in Malaysia in 2014, this did not cause material service disruptions.

Malware – A malware attack involves the use of malicious software to control or disrupt the operations of a targeted system or device. Malware exists in many forms, such as viruses and worms, and can cause harm in different ways. One common form of malware in the context of financial services is the use of spyware installed on unsecured host machines to gather information about the user, which might include his Internet banking login credentials, credit card numbers, or other private or sensitive information. The information is then covertly transmitted back to the attacker for the purposes of committing fraud or other illegal activities (Diagram 2).

Diagram 2

Malware Attack on a Retailer



Source: Bank Negara Malaysia

Phishing – The most common form of fraud, phishing is the use of a fake website to induce an unsuspecting user to divulge sensitive information such as his Internet banking login and credit card details. The stolen information is then used to perform an unauthorised fund transfer or to commit other forms of fraud.

Criminals can combine different techniques to launch sophisticated attacks against systems. For example, malware can be used to take control of a large number of machines in order to carry out a DDoS attack. Such an attack would appear to come from a large number of unrelated sources and be more challenging to defend against. Similarly, by employing malware and phishing techniques, fraudsters can intercept Transaction Authorisation Codes (TAC) and perform fraudulent online banking transactions without the victim's knowledge.

Cyber attacks have also been used in combination with other conventional criminal activities. In 2014, malware was used to gain unauthorised access to 18 on-premise automated teller machines (ATMs) in Kuala Lumpur, Selangor, Johore and Malacca. In these incidents, criminals targeted several poorly guarded ATMs which were based on old models, gaining physical access to the internal components of the ATM and then installing malware into the operating system powering the ATM. The malware was specifically designed to compromise weaknesses in the outdated operating system of the ATMs. This subsequently allowed the criminals to direct the ATM to dispense cash without any authorisation or

[3] Source: Akamai, Arbor Networks.

verification. While the affected banks suffered losses of RM3.4 million, customers were not affected as the withdrawals were not debited from any customer accounts. The affected banks responded swiftly to upgrade the hardware and software of these and other similar ATMs. The banking industry has also since reviewed and implemented enhanced risk management practices and physical security measures to protect ATMs from further threats like these.

As increasingly sophisticated techniques are being employed to launch attacks, identifying and anticipating cyber threats and developing effective counter-measures remains a critical challenge. An organisation might also sometimes be unaware that it is a target of an attack. In what is termed as a `zero-day´ attack, an attacker exploits a vulnerability that is not known to the target, leaving the target no time or opportunity to patch the vulnerability. `Advanced persistent threats´, have also emerged in recent years with the capability to sustain a cyber attack, repeatedly over an extended period of time, while being able to adapt to efforts to resist it.

Industry and Regulatory Response to Cyber Threats

At the national level, initiatives to mitigate cyber security threats in Malaysia are pursued and coordinated with other government agencies as part of the National Cyber Security Framework. Under this national framework, the Bank and the financial institutions it regulates are deemed as Critical National Information Infrastructure (CNII), and thereby subject to heightened safeguards in recognition of their vital role to the country and economy. Important initiatives are pursued to continuously enhance the level of cyber preparedness of CNIIs. This includes annual cyber drills where simulations of cyber-attack scenarios are conducted to test the effectiveness of response programmes of each CNII and all CNIIs collectively against systemic attacks. Results of these exercises are then used to update and improve the response strategies and actions. Several financial institutions have been participating in these cyber drills since 2009 and have successfully completed the exercises by demonstrating the effectiveness of the respective incident response plans in managing the cyber-attack scenarios.

At the industry level, an Internet Banking Task Force (Task Force) established by the Bank and the banking industry supports a comprehensive regulatory response to cyber security threats. The Task Force provides a forum for financial institutions to share intelligence and discuss issues that concern Internet banking, including that on cyber security. Through this Task Force and other platforms, the Bank and the industry engages actively with other government agencies which include the Malaysian Communications and Multimedia Commission, CyberSecurity Malaysia and the Royal Malaysia Police. These engagements enable all stakeholders, including telecommunication companies and Internet service providers, to remain well-informed of latest developments in and emerging threats faced by the financial sector, while continuously promoting the adoption of industry best practices on Internet banking security. For example, the Task Force was instrumental in mitigating the threat of SMS-based scams which were prevalent several years ago. The Task Force shared technical details and information regarding the modus operandi of the scam which enabled weaknesses in the existing processes to be identified and addressed, such as by requiring certain Internet banking customers to register in person at a branch. These measures resulted in a significant decrease in the incidence of SMS-based scams. In its capacity as the competent authority for receiving and analysing information on suspicious transactions, the Bank also disseminates financial intelligence related to persons suspected to facilitate the transaction and mule account holders[4] to support investigations by law enforcement agencies and to reinforce joint efforts in combating cyber crime.

At an institutional level, financial institutions have continued to evolve a wide range of defensive tactics and IT security practices to deter and defend against emerging cyber threats. These include:

- the segmentation of network zones to control user access and limit the propagation of any threats that manage to penetrate the network;
- implementing redundant controls in multiple layers of the network infrastructure (defense-in-depth) so that the failure of one control measure is mitigated by controls in other layers;

[4] People who allow their bank accounts to be used by criminals to hold or transfer money which is acquired illegally.

- deploying appropriate network security tools such as intrusion prevention system (IPS) and the use of multiple firewalls, including the web application firewall (WAF) as an enhanced DDoS mitigation strategy;
- conducting regular and rigorous security assessments on IT infrastructure, including stringent penetration tests. The scope of penetration tests have also been enlarged to include mobile-based applications;
- ensuring constant security monitoring and surveillance to enable the early detection of intrusions; and
- establishing computer emergency response teams to improve response times to cyber incidents.

The effectiveness and consistency of these practices are also regularly reviewed by the auditors of the financial institutions, and any identified weaknesses are promptly highlighted for rectification. Nevertheless, the proper management of cyber security risks is ultimately a board-level responsibility. The Bank expects boards of financial institutions to ensure that sufficient priority and resources are allocated to the oversight and management of these risks. Some boards have already made progress in this area as evidenced by more robust discussions on risk management strategies and a deeper understanding of the more technical aspects of cyber security.

On its part, the Bank had issued various guidelines to specify minimum standards to be observed by financial institutions in the provision of electronic banking services and the management of IT systems and networks. From time to time, these are supplemented by additional guidance published by the Bank to confront specific threats, such as detailed requirements to strengthen security controls on public Internet banking kiosks and to enhance preparedness against DDoS attacks. The Bank is currently in the process of reviewing and updating existing regulatory standards and guidance to further strengthen IT security standards across the financial sector and improve the industry's defense and response to evolving cyber threats. The key objectives of the new standards to be issued in 2015 are to:

- strengthen governance over cyber security in financial institutions;
- ensure that adequate strategic focus and resources are directed by financial institutions at the management of cyber security risks;
- provide practical guidance that reflects the changing technological landscape and business models, and is sufficiently flexible to adapt to new threats;
- increase the rigour of financial institutions' assessment of cyber threats and the quality of information used to inform such assessments;
- further improve recovery plans and contingency or business continuity arrangements; and
- promote more robust due diligence of critical third party service providers.

To ensure that consumers are also able to protect themselves against these cyber threats, efforts have also been directed by the Bank together with the industry, to promote awareness on safe online practices. Aside from continuous consumer education programmes, financial institutions have also stepped-up efforts to provide online banking security tips on their websites.

As existing IT security methods and tools are constantly facing newer threats, the financial sector must remain vigilant against potential vulnerabilities within its critical systems, and continues to update its defenses and strengthen its strategies to mitigate and manage emerging cyber risks. This will include improving intelligence gathering capabilities as well as adopting a more integrated and coordinated approach in dealing with cyber threats.