



The SEACEN Centre

Volume 2 / May 2014

SEACEN FINANCIAL STABILITY JOURNAL

Insights and Thought Leadership
on Financial Stability

What Will Basel III Deliver?

By Stefan Ingves, Governor of the Riksbank and
Chairman of the Basel Committee on Banking Supervision

The Upcoming New Era of Expected Loss Provisioning

Gerald A. Edwards, Jr.

The Mindset and Management for Mastering Financial Stability in the Cyber Frontier

Karl Frederick Rauscher


Consolidated Supervision: Achieving a 360 Degree View of Bank Risk

Mohd Zabidi Md Nor and Michael J. Zamorski

ISSN 2289-6708



9 772289 670007



SEACEN's core membership is comprised of nineteen central banks/monetary authorities in the Asia-Pacific region. SEACEN serves its members through its learning programs, research work, and networking and collaboration platforms for capacity building in central banking knowledge. Through its various activities, SEACEN also strives to promote financial stability in the region, especially through maintaining cooperative relationships and the advocacy of good and best practices in financial institution supervision and central bank policy actions. In addition to its 19 members, it has an outreach of 16 other central banks in the Asia-Pacific region, as well as 26 regional and international strategic partners with which SEACEN collaborates in the design and delivery of its learning programs.

Volume 2 / May 2014

SEACEN
**FINANCIAL
STABILITY**
JOURNAL

Insights and Thought Leadership
on Financial Stability

Editorial Board

The Board of Governors of The South East Asian Central Banks (SEACEN) Research and Training Centre has appointed the following experts on financial stability and related matters to the Editorial Board of the *Journal*:

Dr. Kamalesh Chandra Chakrabarty
Deputy Governor
Reserve Bank of India

Dr. Halim Alamsyah
Deputy Governor
Bank Indonesia

Datuk Nor Shamsiah Mohd Yunus
Deputy Governor
Bank Negara Malaysia

Mr. Nestor A. Espenilla, Jr.
Deputy Governor
Bangko Sentral ng Pilipinas

Dr. Tarisa Watanagase
Former Governor
Bank of Thailand

Mr. Michael J. Zamorski
Adviser
Financial Stability and Supervision
The SEACEN Centre

The Editorial Board has designated Mr. Zamorski as Chief Editor.

CONTENTS

Letter from the Executive Director	... iii
What Will Basel III Deliver? By Stefan Ingves, Governor of the Riksbank and Chairman of the Basel Committee on Banking Supervision	... 1
The Upcoming New Era of Expected Loss Provisioning By Gerald A. Edwards, Jr.	... 13
The Mindset and Management for Mastering Financial Stability in the Cyber Frontier By Karl Frederick Rauscher	... 25
Consolidated Supervision: Achieving a 360 Degree View of Bank Risk By Mohd Zabidi Md Nor and Michael J. Zamorski	... 53

Article Submission Guidelines

The *SEACEN Financial Stability Journal* Editorial Board welcomes potential contributions to the *Journal*. Articles written for the *SEACEN Financial Stability Journal* should focus on providing insights and thought leadership with respect to information and developments relevant and critical to promoting financial stability and related matters, contextualized to the Asia-Pacific region.

- Article drafts should be submitted in 12 point Times Roman font and should be double-spaced, and sent by email to: article@seacen.org.
- The length of draft articles will generally range from 3,000 to 5,000 words (12 to 20 double-spaced typed pages), though treatment of some topics could necessitate longer articles, which would be considered.
- Authors should include a biographical summary at the end of the article. If an article expresses expert opinions, contributors' expert credentials should be apparent.
- Articles will be evaluated by the *Journal's* Editorial Board.
- The Chief Editor and Senior Manager, Communications Unit, are available at any time to answer authors' questions, discuss potential articles, review early drafts, or provide other input. Their Contact details are as follows:

Mr. Michael Zamorski
Tel: +603-9195 1881
Email: mzamorski@seacen.org

Ms. Seow Yun Yee
Tel: +603-9195 1832
Email: yunyee@seacen.org

Letter from the Executive Director

Dear Colleagues and Readers,

We are greatly encouraged by the very favorable reception that the *SEACEN Financial Stability Journal* has received since its launch last October during the celebration of SEACEN's 30th Anniversary. Our goal is to continue to provide our readers with a high-quality, accessible forum for thought leadership and insights in key financial stability-related matters.

I would like to extend a warm welcome to Dr. Tarisa Watanagase, former Governor of Bank of Thailand and career central banker, who was appointed to the *Journal's* Editorial Board by the SEACEN Board of Governors. Dr. Watanagase is a valuable addition to the Editorial Board given her vast knowledge and experience in central banking and financial stability matters. We are most grateful for her willingness to serve.

The Editorial Board has recommended four outstanding original articles for inclusion in this issue of the *Journal*. We are particularly honored that Governor Stefan Ingves of the Riksbank and Chairman of the Basel Committee on Banking Supervision, has contributed an article on Basel III. This new international capital and liquidity standard incorporates important lessons learned from the recent Global Financial Crisis. Countries' sound and timely implementation of Basel III is strongly recommended to enhance the strength and resiliency of their banking systems and help to avert or dampen future crises.

An article by Mr. Gerald Edwards, long-time Chief Accountant of the U.S. Federal Reserve Board and Senior Adviser to the Financial Stability Board, discusses important forthcoming changes in loan loss reserve provisioning standards that will fundamentally alter banks' reserving processes. An article from internationally-renowned cyber security expert, Mr. Karl Rauscher, discusses approaches the financial industry should consider in managing cyber security risks to control related financial and reputational exposure. Additionally, an article co-authored by Mr. Mohd Zabidi Md Nor, Director of Financial Prudential Policy of Bank Negara Malaysia and Mr. Michael Zamorski, Adviser of SEACEN, discusses the importance of achieving effective consolidated supervision of large, geographically-dispersed banking conglomerates to understand and control various types of risks in these typically complex organizations.

I would like to express our sincere gratitude to the Editorial Board members and SEACEN member banks for their valuable input and contributions to this volume of the *Journal*.

Hookyu RHU
Executive Director
25 April 2014

Disclaimer:

The content and views expressed in the SEACEN Financial Stability Journal are solely the responsibility of the authors, and do not reflect the official views, policies or positions of The South East Asian Central Banks (SEACEN) Research and Training Centre or its member central banks and monetary authorities.

What Will Basel III Deliver?

By **Stefan Ingves, Governor of the Riksbank and
Chairman of the Basel Committee on Banking Supervision**

Almost seven years have passed since the start of the global financial crisis. In many parts of the world the after-effects are still being felt. As the causes of the crisis and its fall-out have been thoroughly analysed elsewhere, it suffices to say here that banks with too little equity and too great a reliance on short-term funding proved unacceptably vulnerable to financial shocks. Furthermore, the regulations in force at the time did not adequately capture all the risks to which banks are exposed. In response, the Basel Committee on Banking Supervision (“Basel Committee”) has drawn up Basel III, a new and comprehensive regulatory framework.¹

The development of the Basel III rules is substantially complete, with only a few elements still outstanding. But our job as regulators and supervisors is, in many respects, only just beginning. In this article, I will focus on the intended impact of Basel III’s regulatory reforms once they are fully implemented. I will also discuss what remains to be done to get the most benefit out of the new framework. Overall, Basel III aims to raise the quantity, quality, consistency and transparency of banks’ capital and liquidity positions. In turn, this will deliver a stronger banking system that fosters overall financial system stability, thus providing a foundation for stronger and sustainable growth.

Banking Crises are the Same, Only Different

The lessons from the current crisis are, in many ways, similar to those learned in previous banking crises. One example is the Swedish banking crisis in the 1990s. Then, a fragile banking system characterised by low capital and weak corporate governance, in combination with weak credit extension practices, soaring asset prices and insufficient supervision caused serious problems for the Swedish banks. As a result, five of the six largest banks, comprising close to 85 percent of the banking system’s total assets, failed or came close to failure. Consequently, various forms of public support were needed as well as the involvement of private investors.² In total, the government spent approximately 4 percent of GDP on rescuing the banks.³

More recently, some of the Swedish banks had similar experiences in the Baltic countries. Again, lax credit extension practices allowed low quality assets to build up, leading to major losses when property prices in the Baltics stopped booming. This time, however, although some capital injection was needed at some of the banks, the more evident problem was that the banks relied too heavily on short-term wholesale funding. When the business cycle then turned, investors lost their confidence in Swedish banks. This, in turn, exerted significant pressure on the banks’ liquidity and funding. Close linkages between the banks spread contagion even to those which were less exposed to the region.

The Baltic case also reprised events in several East Asian countries in the late 1990s.⁴ In both these regions, a severe economic crisis, with serious consequences for the banking system, followed a long period of high economic growth, strong credit expansion, prolonged current account deficits, large foreign capital inflows and a dramatic surge in property prices.

While there are many similarities between the regions, there are also major differences. One such difference relates to banks' ownership structures. In East Asia, most of the lending was conducted by locally owned domestic banks, which funded their operations by borrowing from foreign banks. In contrast, banks in the Baltic countries were (and still are) largely foreign-owned, to a large extent by Swedish banks.

All in all, the above examples show that many elements of banking crises are common across geographies and time periods, and often have similar underlying causes. However, differences in market structures, financial shocks, and pre-existing vulnerabilities show that each banking crisis has its own peculiarities and it is not possible to predict all possible triggers or outcomes. It may be true that countries that have previously experienced crises may build up a certain degree of institutional memory that could make them less likely to repeat the experience. But "lessons learnt" will not help every time. This implies the need for an enhanced regulatory and supervisory framework that seeks to deter excessive risk-taking ex ante and to improve overall resiliency to a broader array of shocks.

Basel III Responds to the Global Financial Crisis

The Basel III framework constitutes a central component of the G20 regulatory reforms that followed the 2007/2008 financial crisis. The aim of these reforms is to develop a regulatory framework that better addresses the different risks that banks face and increases the resilience of the banking system. In turn, this will reduce the probability and mitigate the impact of future financial crises.

What can be expected from the Basel III framework when it has been finalised and adopted? More concretely, how will Basel III make the financial system safer? Most regulators and supervisors today agree that no single regulatory measure could have prevented the financial crisis. Therefore, in my view, one of the most important improvements in Basel III is its multi-dimensional approach. Basel III includes four minimum standards: two for capital and two for liquidity.⁵ However, new and strengthened rules are not enough to restore confidence in the banking system. The success of Basel III requires two additional elements. First, the regulatory framework requires sound implementation and oversight, which will enhance its credibility. Second, the framework needs to be transparent and easily understood by stakeholders, hence underpinning market discipline.

Basel III will Increase the Safety Margin of the Financial System

Basel III can be described as a multi-dimensional framework with four cornerstones. The development of the enhanced risk-based capital adequacy framework and the Liquidity Coverage Ratio (LCR) has been completed and these measures are being implemented. In January 2014, the Basel Committee and its governing body, the Group of Governors and Heads of Supervision, took an additional step by agreeing on the definition of a simple, non-risk-based leverage ratio. The fourth cornerstone is the liquidity framework's Net Stable Funding Ratio (NSFR), for which a revised proposal has been published for public consultation with a view to finalising the ratio by the end of this year. Each of these measures will increase the resilience of banks to stress. They also work together to reinforce overall resilience, creating a "virtuous feedback loop" that will help make banking systems safer and sounder.

Strengthening Capital Requirements will Improve Banks' Ability to Absorb Losses

Capital requirements are at the heart of the Basel III framework. Consequently, the main thrust of the Basel III enhancements are reflected in the capital framework. These three major changes have been summed up as "more capital and capital of better quality." Yet, they actually go much further.

First, Basel III introduces higher minimum requirements for regulatory capital by strengthening the quantity, quality and risk coverage of the capital banks hold. The minimum level of Common Equity Tier 1 (CET1) capital in relation to risk-weighted assets (RWA) is increased from 2 percent to 4.5 percent. Equally important, the requirements for the definition of regulatory capital have been tightened. The objective is to ensure that the lion's share of bank capital comprises instruments that are truly loss-absorbing. As a result, a larger part of banks' minimum capital is required to be in the form of equity. This greater loss-absorbing capacity will let a bank continue functioning even when hit by losses.

Second, Basel III introduces two new capital buffers that act as additional "air bags" against losses:

- i) A capital conservation buffer applicable to all banks at all times. This buffer will consist of CET1 capital and must be at least 2.5 percent of RWA.
- ii) A countercyclical capital buffer that requires banks to increase their capital levels in boom years when risks to financial stability tend to build up. The size of this buffer is at the supervisor's discretion but must consist of CET1 capital.

The buffer concept means that, if the banks do not fulfil the requirement, they will be restricted in making any capital distributions such as dividends and bonuses. Hence, the buffers will incentivise banks to increase capital in good times and keep a capital cushion on top of the minimum requirements. The constraints on discretionary

payments also build an automatic corrective mechanism into the regulation, as some (or all) gains have to be retained. The countercyclical buffer gives supervisors a tool to counter the systemic risks arising from very rapid credit expansion. In addition, it introduces a macroprudential measure that not only strengthens bank resilience, but also allows authorities to “lean against” imbalances in the financial system. All told, the total requirement of CET1 capital will be at least 7 percent, and, in some periods, even higher.

Third, there is a further capital surcharge that applies to systemically important banks. The size of this charge depends on a bank’s relative systemic importance, both globally and domestically, and will be met with CET1 capital. The surcharge is meant to ensure that the largest banks have higher loss-absorbency capacity, reflecting the greater impact they have on the financial system. This surcharge, then, tries to address the too-big-to-fail problems observed in the crisis.

As a complement to the risk-weighted capital requirement, Basel III also introduces a leverage ratio. Like the risk-weighted capital measures, the leverage ratio aims to increase banks’ resilience to losses. However, the leverage ratio does not take account of the relative riskiness of a bank’s assets. It is meant to serve as a backstop to the risk-based capital ratios by setting a low floor – currently 3 percent of exposures – that must always be funded by Tier 1 capital.

This is the first time that we have a common global agreement on a leverage ratio and it is an important achievement for the Basel Committee. The leverage ratio has been devised with a view to it migrating to a Pillar 1 minimum requirement. This will be done after appropriate review and calibration, and with consideration given to interactions with the risk-based capital framework. But, as early as next year, banks will have to disclose their leverage ratios according to the definition that the Committee agreed in January.

Basel III also Boosts Banks’ Resilience to Liquidity Shocks

Basel III also introduces two minimum standards to limit liquidity risks. The main motivation is the recent experience of how rapidly even deep markets can become illiquid. The sudden liquidity freezes during 2007/2008 caused severe problems, especially for banks that were heavily dependent on short-term funding. We can all agree that maturity transformation is a key role of banks. However, the overall costs to society of banks’ liquidity stress are often not fully internalised by the banks. But when short-term funding is abundant in supply and relatively inexpensive, banks have private incentives to expand their balance sheets by relying on short-term wholesale funding. This comes at the price of increased vulnerability to liquidity shocks. Therefore, as with the capital requirements, there is a need to limit the risks banks can take.

One of the Basel III measures that addresses liquidity risks is the LCR. It requires banks to hold a buffer of high-quality liquid assets that is large enough to cover their net cash outflows during a stressed scenario lasting 30 days. From the start of implementation

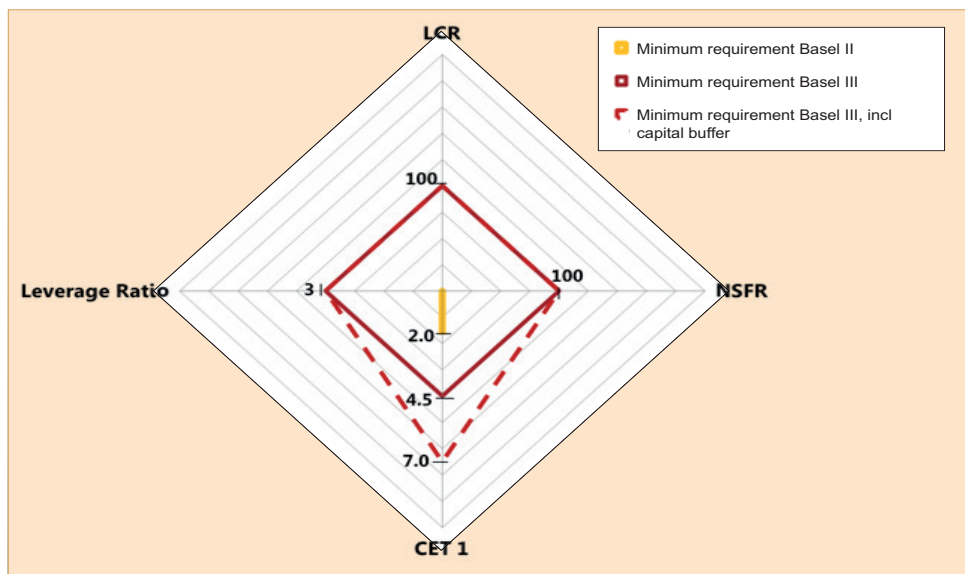
in 2015, the LCR will progressively increase banks’ capacity to resist short-term liquidity stress and disruptions in access to funding. At the same time, the LCR offers options for alternative liquidity treatments that recognise different market structures.⁶

The other Basel III measure to address liquidity risk is the NSFR, which remains to be finalised. The NSFR will encourage banks to maintain more stable and longer-term funding. It does this essentially by placing a ceiling on the maximum maturity mismatch allowed. This will help ensure that banks internalise some of the costs associated with relying on short-term and flighty funding.

A Multi-pronged Approach is Needed

As noted earlier, financial crises can take different forms, some common elements notwithstanding. Basel III therefore seeks to reflect the multi-dimensional perspective on potential risks by examining a bank’s financial health along four axes: capital adequacy, leverage, short-term liquidity and the type and extent of maturity mismatch. This allows us to ensure that banks are robust to a broader spectrum and variety of risks. The four measures also complement each other to reinforce overall bank health and financial system stability. A useful way to illustrate the progress in terms of risk coverage with Basel III is in a cobweb diagram (see Figure 1).

Figure 1. Cobweb Illustration of the Basel Framework



Source: The Riksbank.

Consider, for example, the capital measures. Basel III positions the leverage ratio as a complement to the risk-based framework. Some critics claim that the leverage ratio will unduly punish low-risk banks and incentivise excessive risk-taking, as it looks at banks’ balance sheets without taking into account the riskiness of the business. In

fact, the leverage ratio's lack of risk sensitivity is also its strength. As the leverage ratio does not rely on banks' internal models, it provides an extra layer of protection against model risk and counters attempts to game the risk-based regime. Consequently, the leverage ratio is also a safeguard against risks we cannot envision today. However, a framework that does not adjust for risk is unlikely to be either commercially or socially efficient. Excessive risk-taking would then be constrained by the risk-based ratios. By positioning the leverage ratio as a complement to the risk-based framework, Basel III strives to balance these two aspects.

Furthermore, many regulatory frameworks did not previously include a liquidity standard or did not adequately account for liquidity risk. To some degree, stronger capital positions enhance confidence in banks' solvency, reducing the risk of runs on funding that can lead to liquidity problems. However, the recent crisis showed that meeting the capital requirements was not always sufficient. Inadequate liquidity management and, importantly, contagion effects can create liquidity strains for even strongly capitalised banks. This is particularly true for banks from smaller countries, which are largely dependent on funding from abroad. With the new liquidity standards, the framework covers another dimension of risk.

Referring back to Figure 1, the building blocks of Basel III provide authorities, investors and other stakeholders with tools for identifying imbalances and unsustainable risk-taking in several different dimensions. However, it is important that banks retain their key role as financial intermediaries. Importantly, Basel III does not seek to prevent banks from any and all risk-taking. What it does do is to put limits on the extent to which banks can take excessive risks (i.e., high risk, high leverage, high liquidity risk and high funding risk) in seeking to earn returns for their shareholders. Instead, a multi-dimensional approach to risk management, in my view, creates more effective regulation, fostering growth.

Proper Implementation of Basel III will Strengthen Trust and Confidence in the Banking Sector

The Basel III framework provides an important base for increasing the resilience of banks and fostering financial system stability. However, strengthened regulations alone are not sufficient in the long-run. For any financial system to function well, confidence in the system, in both institutions and authorities, is essential.

The financial crisis seriously hurt confidence in the financial sector, which now has to be restored. To achieve this, at least two conditions need to be met. First, Basel III needs to be consistently implemented. Second, the output of the rules, in terms of reported regulatory ratios, for instance, has to be made transparent to stakeholders.

Implementation of the Rules in a Consistent and Timely Way is Essential

Basel III is intended to transform the landscape of banks' risk management. However, no rule is effective without proper implementation and oversight. Therefore,

consistent and timely implementation of the Basel III framework is a necessary condition for the strengthening of credibility and comparability across institutions and countries. There should be “truth in advertising” for the regulatory ratios that banks present. In order to achieve this, the regulatory framework needs to deliver readily comprehensible and comparable outcomes.

Many banks today are active across international borders. As a globally harmonised framework, Basel III must be consistently implemented if a level playing field is to be achieved and potential market uncertainty to be reduced.⁷ The newly established Regulatory Consistency Assessment Programme (RCAP) started by the Basel Committee in 2012 is one important tool that will underpin consistent and timely implementation.

So far, Basel member jurisdictions are either in the process of implementing or have already implemented Basel III’s risk-based capital framework into domestic regulations.⁸ Some have also started to implement the other parts of the framework. Steady progress is also being made outside the Basel member jurisdictions. For the Asia-Pacific region, the Basel III capital rules are now in force in all of the Committee member jurisdictions and a few have already adopted, or are in the process of adopting, the leverage ratio and the liquidity framework too. Parts of the capital framework are in force in some non-member jurisdictions in the region, or are in the process of adopting the rules. Table 1 below shows an overview of Basel III implementation in the Asia-Pacific region.

Table 1. Basel III Implementation in the Asia-Pacific Region

Status of Basel III Implementation, Number of Countries	Definition of Capital, Risk Coverage and Capital Buffers	Leverage Ratio	D-SIBs Regulations	G-SIBs Regulations ¹	Liquidity Coverage Ratio
Asia-Pacific, total region	18	18	18	8	18
BCBS Member jurisdictions*	8	8	8	8	8
<i>Number of countries where:</i>					
Final rules are in force	8	2	1	2	2
Final rules published, but are not yet in force	0	0	1	0	0
Draft regulations have been published	0	2	2	0	2

Status of Basel III Implementation, Number of Countries	Definition of Capital, Risk Coverage and Capital Buffers	Leverage Ratio	D-SIBs Regulations	G-SIBs Regulations ¹	Liquidity Coverage Ratio
Draft regulations have not been published	0	4	4	2	4
Non-member jurisdictions **	10	10	10	Not applicable (NA)	10²
<i>Number of countries where:</i>					
Final rules are in force	3 ³	0	0	NA	0
Final rules published, but are not yet in force	1	0	0	NA	0
Draft regulations have been published	0	0	1	NA	1
Draft regulations have not been published	6	10	9	NA	9

Note:

* Asia-Pacific BCBS member jurisdictions include: Australia, China, Hong Kong, India, Indonesia, Japan, Korea and Singapore.

** Non-member jurisdictions included in the FSI survey: Bangladesh, Bhutan, Fiji, Macau, Malaysia, Nepal, New Zealand, Philippines, Sri Lanka, and Thailand.

1. G-SIB regulations are not applicable to some of the BCBS member jurisdictions in this region at present and none of the non-member jurisdictions.
2. Of these, one jurisdiction was not planning to implement the Basel LCR regime as it already had a somewhat similar regulation in place.
3. In these jurisdictions, the regulations implementing other elements of Basel III capital standards (risk coverage, the capital conservation and countercyclical capital buffers requirements) are in the process of being adopted.

The Regulatory Framework has to Deliver Understandable and Comparable Outputs

Nonetheless, studies by the Basel Committee have shown that variations in the regulatory ratios still exist, even when the rules are implemented consistently. For example, when banks use internal models, there are unacceptably large variations in the outcomes of RWA calculations both across a global sample and within the same country. This erodes both the credibility of capital standards and their comparability across banks, hence undermining market discipline.

One line of action currently under discussion is to assess whether the framework can be simplified in some respects. Overly complex standards are hard to understand and explain, thus reducing comparability when implemented and opening the door to regulatory arbitrage. In addition to eliminating or reducing overly complex elements, the use of complementary measures – such as the leverage ratio – may increase comparability.

No less important is transparency, which can be improved through improved public disclosure. The provision of meaningful information on key risk metrics reduces information asymmetry, both in benign and stress periods, as illustrated by the classical lemons problem.⁹ Moreover, transparency facilitates market discipline, which can help reduce excessive risk-taking ex ante if banks know that market participants will penalise this type of behaviour. Increased requirements on the public disclosure of risk metrics, including the use of common templates, increased minimum reporting frequency and standardised definitions, are all part of the Basel III framework. Concrete examples include the disclosure frameworks for the LCR and the leverage ratio. In addition, the Basel Committee will issue a proposal for a revised Pillar III framework for public consultation later this year. The proposal includes welcomed improvements on earlier versions of the Basel framework with respect to both the way disclosures are presented and their content. The Basel Committee also intends to tighten the requirements on the disclosure of RWA information.

While there are concerns that public disclosure could have adverse effects, particularly during periods of stress, the Swedish experience indicates otherwise. One concrete example relates to the Baltic crisis mentioned earlier. To reduce uncertainty about the extent of the problems, the Riksbank published stress test results of individual banks. Once it was clear how large the potential losses might be and how much capital support could be needed under an adverse scenario, investors could see the degree of stress at individual banks in relation to the broader banking system. In my view, this contributed to reducing the indiscriminate rise in risk aversion towards all Swedish banks, easing systemic stress. Those banks that were truly under strain were still “punished” by the markets, but the negative market reaction was potentially less severe than it would have been had the extent of problems remained uncertain. This example and the previous illustrate an important point: banks pay an uncertainty risk premium when raising funds; the higher the transparency about exposures and risks, the lower the uncertainty premium.

Similarly, in December 2010, the Riksbank started to publish information about the liquidity ratios of Swedish banks. Evidence indicates that these disclosures have improved confidence in the Swedish banks by alleviating some of the market uncertainty. Eventually, adhering to the recommendation of the Riksbank, the banks started to disclose their liquidity ratios themselves. In retrospect, increased disclosure appears to have enhanced banks’ motivations to adopt a more long-term strategy to manage liquidity risks, particularly to improve their liquidity ratios, illustrating the beneficial impact of market discipline and promoting confidence in the Basel III framework.

Conclusion

Experience shows that a similar set of features tends to recur in every financial crisis. These shared characteristics extend to both the underlying causes and the factors that shape how a typical crisis evolves. At the same time, each banking crisis has its own special features and, as a corollary, it will never be possible to predict each and every melt-down.

Basel III therefore takes a multi-dimensional approach to addressing banks' risks. Under the new framework, banks will be better capitalised and their balance sheets less leveraged. Liquidity risk management will be improved and funding profiles more stable. If the framework is consistently implemented, with appropriate transparency and disclosure, Basel III will reduce uncertainty and strengthen confidence in the banking system. This is the promise of Basel III. As the Basel Committee finalises the few remaining policy aspects of the framework and through our focus on consistent implementation, we are helping to ensure that this promise will be fulfilled.

Nonetheless, there are still things that need to be done if Basel III is to realise its full potential. Some of these tasks must be shouldered by the Basel Committee. They include, for instance, continuing to seek the right balance between simplicity, risk-sensitivity and comparability in the standards. The Committee also needs to keep studying ways of increasing the reliability of risk weights and tightening the requirements that govern internal models. This work will be complemented by the Committee's efforts to foster meaningful cooperation between authorities through supervisory dialogue and outreach. Other tasks must be taken on by the jurisdictions, in particular, the responsibility for timely and consistent implementation of the Basel III framework. It is the jurisdictions too that will oversee the outcome in banks' internal risk management practices.

This may not always be the easiest path to walk. Especially in today's economic environment, we must recognise that implementing the standards will often pose challenges in the short-term. But that does not mean that we should delay the reforms. Rather, we should push ahead and do the repair work that needs to be done, as soon as possible. Reforms are often seen as imposing costs; I prefer to think of them not as costs, but as investments in a more stable future. In any event, banks with weak capital positions and insufficient liquidity buffers cannot conceivably borrow and lend in the way we want them to. That is obvious in markets like Asia, where strongly capitalised banks were less affected by the crisis, and are now stepping into markets that are being vacated by banks that were over-leveraged. Strong banks can finance economic activity, weak banks cannot. Indeed, enhancing the strength of the banking system will better provide a foundation for sustainable competition and durable growth.

Endnotes

1. The Basel framework is comprised of three Pillars. Pillar I involves the minimum quantitative requirements for regulatory capital and liquidity. Pillar II, the supervisory review process, covers risk management and supervision and Pillar III relates to market discipline and sets out minimum requirements for disclosure. See www.bis.org/bcbs/basel3/b3summarytable.pdf.
2. For example, one bank was put into liquidation while others were restructured and merged. Large amounts of bad loans were transferred to a public asset management corporation, a so-called “bad bank.”
3. Corresponds to the total amount contributed to the banks by the Swedish government during the crisis in relation to the Swedish GDP in 1993.
4. See Bernhardtson, Ellen and Billborn, Jill, (2013), “The Role of the Banking System in Financial Crises – a Comparison between the Crisis in Asia and the Crisis in the Baltic Countries,” *Economic Review*, 1, Sveriges Riksbank and Bonte, Rudi, (1999), “Supervisory Lessons to be Drawn from the Asian Crisis”, *BCBS Working Papers*, No. 2, June, BIS.
5. This article focuses on the regulatory reforms in Basel III. However, the Committee is working on a number of other reforms, of which many was initiated following the crisis that will also strengthen the financial system in different ways. Those are, for example, a fundamental review of the trading book, a review of the capital framework for securitization and a number of reforms related to the market for OTC derivatives.
6. These alternatives include: (i) the option to use contractual committed liquidity facilities from central banks subject to certain conditions; (ii) the use of foreign currency High Quality Liquid Assets, HQLA, to cover domestic liquidity needs and (iii) the potential use of certain high quality liquid assets with a higher haircut.
7. For example, differences in the definitions of core capital across jurisdictions raised concerns about the true state of some banks’ health.
8. The latest progress report on the implementation of the Basel regulatory framework, from October 2013, can be found at <http://www.bis.org/publ/bcbs263.pdf>.
9. The lemons problem was described by Akerlof in 1970. The lemons problem illustrates the information asymmetry that exists between a seller and a buyer of a product. The buyer will weigh in the risk of buying a bad product when deciding what he is prepared to pay, meaning that he will not be prepared to pay more

than the average value of the products available in the market. Akerlof, George A., (1970), "The Market for 'Lemons': Quality Uncertainty and the Market Mechanism," *Quarterly Journal of Economics*, 84 (3).

The Upcoming New Era of Expected Loss Provisioning

By Gerald A. Edwards, Jr.*

The global financial crisis highlighted the need for significant improvements in the financial reporting of credit losses on loans and other financial instruments held by banks and other companies. After calls for action by the G20 Leaders, investors and other users, regulatory bodies and prudential authorities, the International Accounting Standards Board (IASB) and the U.S. Financial Accounting Standards Board (FASB) have nearly completed the development of new approaches for loan impairment based, for the first time, on an expected loss model. The new loan impairment standards will be finalized and published later this year. Once effective, they are expected to result in a significant rise in the level of provisioning for many banks.

Before introducing the new IASB and FASB expected loss approaches, this article summarizes key efforts of the G20, Financial Stability Board (FSB and its predecessor, the Financial Stability Forum, or FSF) and Basel Committee on Banking Supervision (BCBS) that encouraged the development of these new standards. The article then explores the potential impact of the new standards and the challenges that will be faced by prudential authorities, including in the Asia-Pacific region.

Encouragement to Consider Expected Loss Provisioning

Under both IASB standards (called International Financial Reporting Standards or IFRS) and FASB standards, the accounting model for recognizing credit losses is commonly referred to as an “incurred loss model” because the timing and measurement of losses is based on estimating losses that have been incurred as of the balance sheet date. Provisioning requirements in IASB and FASB standards thus generally limit provisioning to losses that are considered probable as of the balance sheet date. In addition, these accounting standards do not permit credit losses based on events that are expected to occur in the future to be included in provisions until the event or events that would probably result in a loss have occurred, generally supported by observable evidence (e.g., borrower loss of employment, decrease in collateral values, past due status). These events are sometimes referred to as “triggering events.”

While the incurred loss model had been ingrained in the thinking of standard-setters for many years, the experience of the financial crisis highlighted the delayed recognition of credit losses caused by the incurred loss standards which, during the “good years” before crises, preclude banks from provisioning appropriately for credit losses likely to arise from emerging risks. These delays resulted in the recognition of credit losses that were widely regarded as “too little, too late.” Moreover, questions were raised about whether the incurred loss model contributed to procyclicality.

In its April 2008 Report in response to the request of the G7,¹ the FSF noted that it would examine the forces that contribute to procyclicality in the financial system and develop options for mitigating it. At the G20 Leaders Summit in London in April 2009, the FSF issued a report, “Addressing Procyclicality in the Financial System.”²

The term “procyclicality” refers to the dynamic interactions between the financial and the real sectors of the economy. These mutually reinforcing interactions tend to amplify business cycle fluctuations and cause or exacerbate financial instability. The global financial crisis was a graphic example of the disruptive effects of procyclicality. Institutions that experienced extensive losses faced growing difficulties in replenishing capital. This, in turn, induced them to cut credit extension and dispose of assets. Their retrenchment precipitated a weakening of economic activity, thereby raising the risk of a further deterioration in their financial strength. Addressing procyclicality in the financial system is an essential component of strengthening the macroprudential orientation of regulatory and supervisory frameworks.

The FSF report examined the forces that contribute to procyclicality in the financial system, and explored possible mitigating actions in three main areas: (i) the Basel II capital accord; (ii) loan loss provisioning; and (iii) valuation and leverage. The recommendations in the report were the result of collaborative work involving national authorities, the BCBS, Bank for International Settlements, Committee on the Global Financial System, International Monetary Fund, International Organization of Securities Commissions (IOSCO), the IASB and the U.S. FASB.

New thinking was needed, based on lessons from the financial crisis, to reform the accounting model for loan losses in a manner that would support the overall goal of improving transparency. To carry forward its analysis on the need for provisioning improvements, the FSF formed a new Working Group on Provisioning, co-chaired by Kathleen Casey, Commissioner, U.S. Securities and Exchange Commission, and Chairman of IOSCO’s Technical Committee, and by John Dugan, U.S. Comptroller of the Currency and Joint Forum Chairman. This working group brought together securities regulators, banking supervisors, accounting standard-setters and audit regulators to evaluate this key area. Both U.S. and international perspectives were carefully explored. The IASB and FASB were fully involved, as were BCBS representatives and the chairmen of the International Forum of Independent Audit Regulators and the U.S. audit regulator, the Public Company Accounting Oversight Board. The working group also engaged in outreach involving investors, external auditors and financial institutions. This effort helped to ensure that the group’s findings would address the needs of investors while also addressing certain key prudential objectives.

In April 2009, based on the working group’s recommendations, the FSF’s procyclicality report to the G20 noted that: “Earlier recognition of loan losses could have dampened cyclical moves in the current crisis. . . . Earlier identification of credit losses is consistent both with financial statement users’ needs for transparency regarding changes in credit trends and with prudential objectives of safety and soundness.” The FSF report recommended: “The FASB and IASB should reconsider the incurred loss model by analyzing alternative approaches for recognizing and measuring loan losses that incorporate a broader range of available credit information.”

At the London summit meeting in April 2009, the FSF was re-established as the FSB with a broadened mandate to promote financial stability. The G20 Leaders

welcomed the accounting recommendations in the FSF's procyclicality report and requested action by accounting standard-setters.³ The G20 Leaders also called on "the accounting standard setters to work urgently with supervisors and regulators to improve standards on valuation and provisioning and achieve a single set of high-quality global accounting standards."⁴ Specifically, the G20 Leaders encouraged accelerated efforts by the IASB and FASB to finalize improved, converged accounting standards and efforts to enhance the governance of the IASB.

The G20 Leaders requested that the FSB monitor implementation efforts, including those addressing accounting issues. Starting with its progress reports to the G20 Leaders in September 2009, the FSB has included recommendations on accounting matters in its communications with the G20, including an assessment of IASB-FASB convergence progress. In its progress report to the G20 Leaders in September 2009, the FSB noted that, "We are particularly supportive of continued work on impairment standards based on an expected loss model."⁵ The IASB Chairman, who is a member of the FSB, has periodically updated the FSB on IASB efforts to address accounting recommendations of the G20 and the FSB. The FASB Chairman also provided updates to the FSB on FASB's convergence program. These included updates that were discussed at FSB meetings on IASB and FASB efforts to enhance and converge their standards on loan loss provisioning and the valuation of financial instruments. Moreover, as part of a joint approach to address the reporting issues arising from the global financial crisis, the IASB and FASB formed the Financial Crisis Advisory Group (FCAG) in October 2008 and asked FCAG to consider how improvements in financial reporting could help enhance investors' confidence in financial markets. FCAG's members were senior leaders with broad international experience in the financial markets and were joined by participating official observers representing the FSB, BCBS and key global banking, insurance and securities regulators. In July 2009, the FCAG report identified delayed recognition of losses associated with loans (and other financial instruments) and the complexity of multiple impairment approaches for different types of financial assets as primary weaknesses in accounting standards and their application. The FCAG report included a recommendation that the IASB and FASB explore alternatives to the incurred loss model that would use more forward-looking information.

In addition, in 2009 the BCBS formed the High Level Working Group on the G20 Accounting Recommendations (HLWG) to assist the BCBS in developing approaches to provisioning, fair value accounting and other accounting recommendations of the G20 and to work with the IASB in this respect.⁶ The HLWG also worked closely with the BCBS Accounting Task Force with regard to these matters. In August 2009, based on the work of the HLWG the BCBS issued for consideration by accounting standard setters principles for the revision of accounting standards for financial instruments, agreed by all G20 banking supervisors. These BCBS principles encouraged improved standards for provisioning based on expected losses, as well as enhanced guidance for fair value measurement and related disclosures.⁷ The BCBS, through its HLWG and Accounting Task Force also met periodically with IASB officials and provided comment letters to the IASB on its proposed standards in order to encourage progress in improving IASB standards in these key areas.

This encouragement from the G20 Leaders, FSB, BCBS, FCAG and key regulatory bodies, together with investor support for a move to an expected loss model, was followed by valuable work by the accounting standard setters. The IASB proposed an expected loss impairment or provisioning model in November 2009. The FASB, after first proposing in May 2010 a modified version of the incurred loss model, worked jointly with the IASB starting in early 2011 on clarifying an expected loss impairment approach. The IASB and FASB subsequently published a joint proposal in 2011 and through July 2012 they continued to develop a common impairment approach based on expected losses. However, in August 2012, FASB decided to amend the common impairment approach to simplify the expected loss measurement objective and address concerns that had been expressed by U.S. investors, preparers, auditors and regulators, and it published this revised expected loss model as an exposure draft in December 2012 for public comment. The IASB published its proposed expected loss model in an exposure draft in March 2013. These proposals are summarized below.

The IASB Expected Loss Impairment Approach⁸

The IASB expected loss impairment approach would be part of IFRS 9, *Financial Instruments*. In summary, all banks and other companies that hold financial assets or commitments to extend credit that are not accounted for at fair value through profit or loss (e.g., trading portfolios) would be affected by this proposal. This includes loans and other financial assets measured at amortized cost or that are reported at fair value through other comprehensive income (similar to today's available-for-sale assets), trade receivables and lease receivables, loan commitments and financial guarantee contracts.

Under the proposal it would no longer be necessary for a credit event to have occurred before credit losses are recognized. Instead, expected credit losses and changes in expectations regarding credit losses would be recognized and would be updated at each reporting date to reflect changes in credit quality.

Under the IASB proposal banks and other companies would report expected credit losses in three stages as deterioration in credit quality takes place after initial recognition of the loan. For stage 1, they would report 12-month expected credit losses and for stages 2 and 3, full lifetime expected credit losses would be reported.⁹

Stage 1. As soon as a financial instrument is originated or purchased, 12-month expected credit losses would be reported in profit and loss and an allowance for expected credit losses (loss allowance) or provision would be established. This would serve as a proxy for the initial expectations of credit losses that are priced into the financial instrument. For loans or other financial assets, interest revenue would be calculated on the gross carrying amount of the financial asset (i.e., without adjustment for the loss allowance).

A bank or other company would calculate "12-month expected credit losses" by multiplying the probability of a default occurring in the next 12 months by the total (lifetime) expected credit losses that would result from that default.

Stage 2. When the credit risk increases (or credit quality deteriorates) significantly and the resulting credit quality is below “investment grade,” full lifetime expected credit losses would be reported (if the credit quality deteriorates significantly from that at origination or purchase).¹⁰ The calculation of interest revenue on financial assets remains unchanged from the approach set forth for Stage 1.

Stage 3. This stage occurs when the credit quality of a financial asset deteriorates to the point that credit losses are incurred or the asset is credit-impaired. Interest revenue is then calculated based on the net amortized cost carrying amount (i.e., the gross carrying amount adjusted for the loss allowance). Lifetime expected credit losses would continue to be reported for loans in this stage of credit deterioration.

Under the IASB proposal, lifetime expected credit losses – reported for stages 2 and 3 -- are an expected present value measure of credit losses that arise if a borrower defaults on its obligation throughout the life of a financial instrument. They are the weighted average credit losses with the respective probabilities of default as the weights. Because the measure of credit losses is a present value, a credit loss may result from a delay in the payment of contractually required amounts, even if full repayment of those amounts is expected. Banks and other companies should base their measurement of expected credit losses on relevant information about past events, including historical credit loss events for similar financial instruments, current conditions and reasonable and supportable forecasts.

Thus, the IASB approach recognizes a portion of the lifetime expected credit losses, and then the full lifetime expected credit losses only after significant deterioration in credit quality is expected. The IASB believes that this approach ensures more timely recognition of expected credit losses than the existing incurred loss model; distinguishes between financial instruments that have significantly deteriorated in credit quality and those that have not; and better approximates economic expected credit losses.

The IASB exposure draft proposes extensive disclosures about expected losses and changes in the credit risk of the loan portfolio and other financial instruments subject to its impairment approach.

The IASB has tentatively completed its consideration of comments received on the exposure draft and will proceed with the proposed expected credit loss impairment model that is based on 12-month and lifetime expected credit losses, with certain refinements in response to comments. The IASB plans to provide further clarification, application guidance and illustrative examples, to help banks and other companies with implementation. The completed version of IFRS 9 *Financial Instruments*, including classification and measurement, expected loss impairment, and hedge accounting requirements, is expected to be issued by the IASB in the second quarter of 2014 and would be effective for annual periods beginning on or after 1 January 2018.

The FASB Expected Loss Impairment Approach¹¹

As previously mentioned, the IASB's "three-stage" or "three-bucket" impairment model utilizes two different measurement objectives – 12-month expected losses and lifetime expected losses -- to determine the credit impairment for the financial asset, depending on the extent of credit deterioration (or recovery) since it was originated or acquired. During FASB's outreach with users, preparers, auditors, and regulators, it heard significant concerns that the three-stage/bucket impairment model would not be understandable, operable, or auditable. For example, many were confused about how to determine when financial assets should be "transferred out" of Stage 1/bucket 1 (12-month expected losses) and be reported as experiencing credit quality deterioration under Stage 2/bucket 2 or Stage 3/bucket 3 (both reporting lifetime expected losses). In addition, many stakeholders viewed the proposed "transfer criteria" as reintroducing an incurred loss recognition "trigger", which was one of the primary problems identified with the existing impairment model. Finally, some stakeholders expressed concern that the allowance for expected credit losses may not reflect the appropriate amount of risk in the organization's asset portfolio, taken as a whole, considering that historically most loans would be categorized as in Stage 1/bucket 1.

As a result, the FASB exposure draft does not use the IASB's three-stage model but instead sets forth a "current expected credit loss" (CECL) model. This model would replace the multiple impairment models that currently exist for loans and other debt instruments in U.S. generally accepted accounting principles (GAAP). The CECL model uses a single "expected credit loss" measurement objective for the allowance for credit loss. Under this model, the allowance for expected credit losses would reflect management's current estimate of the contractual cash flows that the company does not expect to collect, based on its assessment of credit risk as of the reporting date.

This model removes the "transfer criteria" trigger in the IASB's three-stage model that U.S. stakeholders indicated was inoperable and might inhibit the timely recognition of credit losses. Furthermore, this model considers more forward-looking information than is permitted under current U.S. GAAP. When credit losses are measured under current U.S. GAAP, a bank or other organization generally only considers past events and current conditions in measuring the incurred loss, but the CECL model also would require consideration of reasonable and supportable forecasts that affect the expected collectibility of the financial assets' remaining contractual cash flows. That estimate would be neither a "worst case" nor a "best case" scenario, but rather would reflect management's current estimate of the contractual cash flows that the organization does not expect to collect.

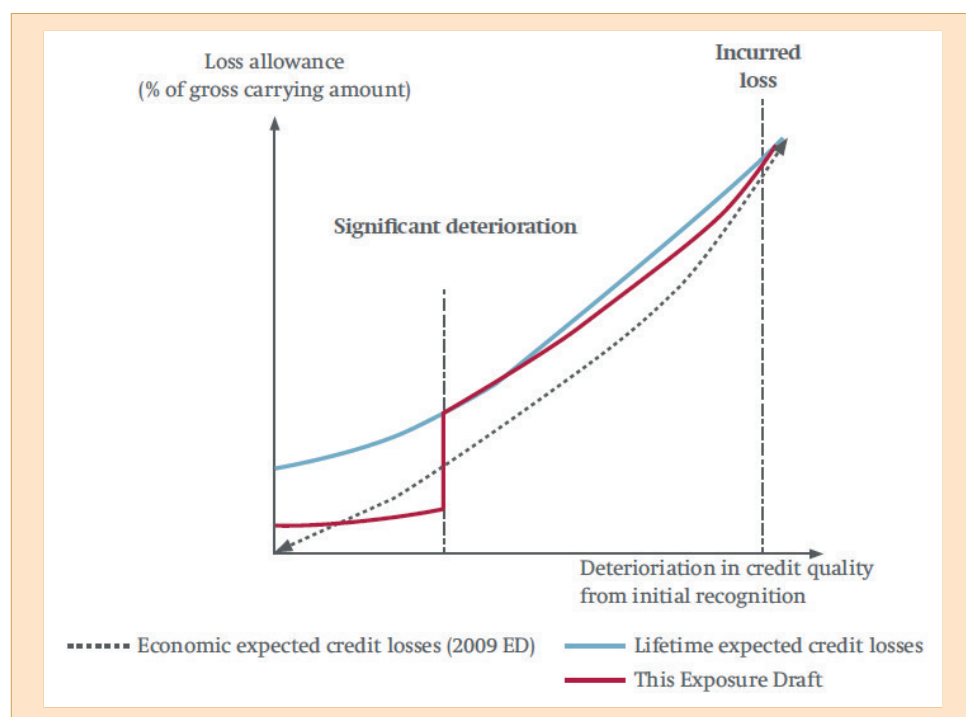
Thus, the balance sheet would reflect the current estimate of expected credit losses over the remaining life of a loan portfolio at the reporting date and the income statement would reflect the effects of credit deterioration (or improvement) that has taken place during the period.¹² The proposal also includes disclosures about expected credit losses and changes in credit risk.

The FASB is continuing its discussions about possible refinements to the CECL model based on consideration of comments on the exposure draft and it expects to issue the final standard in the second half of 2014. The effective date of the standard has not yet been determined.

Potential Impact of the New Standards

It is difficult to estimate precisely the potential impact of the IASB and FASB expected loss provisioning approaches on bank loan loss allowances before the final standards are issued and effective. However, Hans Hoogervorst, IASB Chairman, when discussing the IASB impairment model in a speech in December 2013, stated that, “Our field work shows that it will lead to a significant rise in the level of provisioning.”¹³ Moreover, Thomas Curry, U.S. Comptroller of the Currency, in a speech at a major banking conference in September 2013, said, “There is no question that implementation of the FASB proposal will require most banks to boost their allowance. But the OCC’s impact analysis showed that the increases would be far more modest [than some industry estimates of 200 – 300 percent] – perhaps in the neighborhood of 30 to 50 percent system-wide if applied today. For some banks it will be more; for others, less depending on the loan portfolio and environment at the time of implementation.”¹⁴

Figure 1



Source: IASB Snapshot: “Financial Instruments: Expected Credit Losses,” (Exposure Draft), March 2013.

As previously mentioned, when expressing its support for an impairment approach based on expected credit losses, the FSB recommendations to the IASB and FASB in 2009 called for loan impairment approaches to (a) incorporate a broader range of available credit information and (b) result in an earlier recognition of loan losses than under the incurred loss model. The FSB procyclicality report found that these provisioning qualities should improve transparency to investors while also mitigating procyclicality. The IASB-FASB FCAG had also called for impairment approaches to use more forward-looking information. Figure 1, from the IASB, illustrates that expected loss impairment approaches should result in earlier recognition of credit losses than under the incurred loss impairment model. In Figure 1, the red line approximates the recognition of credit losses under the IASB's expected loss approach (12-month expected losses for loans in Stage 1, followed by lifetime expected losses for loans experiencing significant credit quality deterioration in Stages 2 and 3). The blue line in Figure 1 approximates the way that the FASB expected loss approach (essentially, "lifetime expected losses") would recognize credit losses. Assuming robust forward-looking estimates, both impairment approaches would recognize credit losses well before they would be reported under the incurred loss model (the right-most black vertical "dashed" line in Figure 1). Thus, the IASB and FASB new impairment approaches could be among those practices that help mitigate procyclicality.

Officials from the FASB, IASB, the banking industry, and prudential authorities have noted that the FASB approach will likely result in more "upfront" recognition of expected credit losses than the IASB approach. This can be seen in Figure 1, as the blue line (the FASB approach, essentially, "lifetime credit losses") initially exceeds the red line (the IASB 12-month expected credit losses under Stage 1) until serious credit quality deterioration occurs (at which point, in Stages 2 and 3, the IASB approach also requires use of lifetime expected credit losses). However, given the robust nature of U.S. banks' current loan loss provisioning practices, some U.S. stakeholders have expressed concern that the new IASB three-stage impairment approach could lead to a significant reduction in loan loss allowances at U.S. financial institutions if it were adopted in the U.S.¹⁵

Due to the forward-looking nature of the new impairment approaches, many banks are likely to see a significant impact from the applicable standards, and may need additional systems and processes to collect the necessary forward-looking information about credit risk. For example, the IASB and FASB standards will require consideration of forecasts and their effect on the expected collectibility of the financial assets' remaining contractual cash flows, and bank management must determine which forecasts are reasonable and supportable for this purpose. This aspect alone could result in a significant increase in the number and complexity of management judgments that would be needed to determine the adequacy of expected loss provisions, which could also contribute to challenges for investors, auditors, and supervisors in assessing provisioning levels and practices. Moreover, banks will need to ensure that their risk management systems, including their internal credit risk grading frameworks, appropriately interface with their accounting systems so as to result in robust expected loss provisioning practices and useful risk disclosures.¹⁶

The BCBS, through its Accounting Expert Group (formerly, the Accounting Task Force), has maintained extensive periodic dialogue with the IASB, FASB, the global banking industry and bank audit firms about the IASB and FASB expected loss approaches. In addition, the BCBS has carefully monitored the IASB and FASB proposals and provided technical comment letters to the boards. After the IASB and FASB final standards are published, the BCBS will consider issuing enhanced supervisory guidance that will address key issues associated with the standards and how supervisors can evaluate expected loss provisioning practices and encourage their banks to maintain sufficient levels of provisions, consistent with a robust expected credit loss impairment model.¹⁷ In addition, the Federal Reserve Board and the other U.S. federal banking agencies have been providing comments to the FASB on its planned CECL impairment standard and are likely to issue supervisory guidance to enhance the provisioning practices of U.S. banking organizations once the final FASB standard is issued and effective.

The potential impacts of the new impairment standards will be important for leaders in Asia-Pacific region to carefully evaluate. Research has highlighted that after the Asian financial crisis, many countries in the Asia-Pacific region enhanced their loan loss provisioning requirements by adopting international standards and overlaying these with prudential rules and other requirements that sought to increase provisioning in good times in response to rising levels of credit risk. These requirements have also led to bank provisioning practices that have tended to be countercyclical in nature in many Asian jurisdictions, for example, in emerging Asia.¹⁸ Care must be taken by prudential authorities so that implementation of the new IASB expected loss provisioning standard will improve transparency while also building on progress in achieving important prudential objectives.¹⁹ For example, under the new expected loss provisioning standards, prudential authorities will need to understand and address whether the following may be needed:

- Revisions to their current national provisioning matrices or other requirements that have contributed in the past to robust provisioning levels (e.g., improved consideration of qualitative factors and other forward-looking information affecting the collectability of loans);
- New guidance on the interrelationship between capital adequacy and expected loss provisioning (e.g., given the different time frames for loss coverage underlying expected losses for capital and financial reporting purposes);
- New guidance on appropriate internal controls, including internal audit and internal credit review procedures, and tests of controls to assess and strengthen banks' internal control systems associated with expected loss provisioning and related risk disclosures; and
- Enhancements to regulatory financial reports that banks provide to prudential authorities and macro-prudential analyses developed for offsite monitoring purposes.

As banks prepare to implement the new expected loss provisioning requirements and their auditors gear up to assess them, supervisors will also need to understand these developments and design new procedures to ensure that banks' new provisioning systems truly capture emerging risks.

The upcoming new era of expected loss provisioning will not guarantee a future free of financial crises. However, implementation of the new IASB and FASB impairment standards should improve transparency to investors and help banks' financial reporting of credit losses to better reflect the risks retained in their loan portfolios in ways that should mitigate procyclicality. Working with the banking industry and auditors, prudential authorities can have an important role in helping to secure the potential benefits of the new expected loss provisioning regime.

* **Gerald A. Edwards, Jr.** has held important positions with both the U.S. Federal Reserve Board and the Financial Stability Board. He retired in 2013 with over 30 years experience from the U.S. Federal Reserve Board's Division of Banking Supervision & Regulation in Washington, DC, USA, where he most recently held the official position of Senior Adviser and had served earlier as Associate Director and Chief Accountant. Previously, from mid-2005 to end-2012, he served as Senior Advisor on Accounting and Auditing Policy with the Financial Stability Board (FSB, and its predecessor, the Financial Stability Forum), with a dual senior advisory role with the Basel Committee's Accounting Task Force, at the Bank for International Settlements (BIS) in Basel, Switzerland. He was heavily involved in the international efforts to address the global financial crisis and its aftermath and participated in the development of international policy recommendations to promote financial stability. He also co-chaired the Basel Committee's High Level Working Group on the G20 Accounting Recommendations from 2009 to 2012. He also served as the FSB's representative on the IASB-FASB Financial Crisis Advisory Group and on other key accounting and auditing advisory groups.

Endnotes

1. “Report of the Financial Stability Forum on Enhancing Market and Institutional Resilience,” April 2008.
2. See www.financialstabilityboard.org/publications/r_0904a.pdf.
3. G20 Leaders, “Declaration on Strengthening the Financial System – London Summit, 2 April 2009.”
4. G20 Leaders, “London Summit – Leaders’ Statement, 2 April 2009.”
5. “Improving Financial Regulation, Report of the Financial Stability Board to G20 Leaders”, September 2009.
6. The HLWG was active from 2009 to 2012 and was co-chaired by the chair of the BCBS Accounting Task Force and the author of this article.
7. “Guiding Principles for the Replacement of IAS 39,” BCBS, August 2009. In a letter to the chairs of the IASB and FASB in December 2012, the BCBS updated these principles with respect to loan impairment and reiterated the BCBS’ support for use of a converged approach to impairment based on expected losses.
8. IASB Snapshot: “Financial Instruments: Expected Credit Losses,” (Exposure Draft), March 2013.
9. These stages were previously referred to as “buckets” in some earlier summaries of the IASB expected loss impairment approach, leading some to refer to the IASB approach as the three-bucket impairment model.
10. This requirement for significant credit risk deterioration before a loan can be reported under Stage 2 is sometimes referred to as the “transfer criteria” to move from Stage 1 (12-month expected credit losses) to Stage 2 (lifetime expected credit losses).
11. FASB in Focus: “Proposed Accounting Standards Update – *Financial Instruments – Credit Losses (Subtopic 825-15)*”, 20 December 2012.
12. In contrast, the IASB does not believe that the FASB’s proposed approach to recognizing lifetime expected credit losses on loans faithfully represents economic expected credit losses. The IASB believes that the FASB’s approach results in: (a) the double-counting of expected credit losses that are priced into a loan; (b) a loss of information about the changes in credit quality (i.e., it may not be apparent whether losses recognized represent an economic loss, or will be compensated by

- future interest revenue); and (c) in loans having carrying amounts (net of their credit loss allowance) that would be below their fair value or transaction price on initial recognition.
13. “Why the Financial Industry is Different: *The Relevance of Current Measurement for the Financial Industry*,” Speech at the Joint ICAEW and IFRS Foundation Financial Institutions IFRS Conference, by Hans Hoogervorst, London, 3 December 2013.
 14. Remarks by Thomas J. Curry, Comptroller of the Currency, before the AICPA Banking Conference, Washington, D.C., 16 September 2013.
 15. For example, see summary of FASB discussions at the Financial Executives International (FEI) blog, “FASB Credit Loss Model CECL Could Drive 20-50% Increase in Allowances: FASB, OCC Studies,” September 2013.
 16. Many large banks are implementing the recommendations of the FSB’s Enhanced Disclosure Task Force, issued in October 2012, in order to improve their risk disclosure practices and transparency to investors. See http://www.financialstabilityboard.org/press/pr_121029.pdf.
 17. In view of the difference between expected losses under the Basel Capital Framework and the IASB and FASB expected loss provisioning standards, it also may be helpful for BCBS guidance to address this.
 18. Frank Packer and Haibin Zhu, (2012), “Loan Loss Provisioning Practices of Asian Banks,” *BIS Working Paper*, No. 375, April.
 19. This will be particularly important if surveys or other analyses indicate that the level of provisions of certain banks might be reduced when implementing the final IASB expected loss provisioning standard.

The Mindset and Management for Mastering Financial Stability in the Cyber Frontier

by Karl Frederick Rauscher*

1. Introduction

Cyber security is rapidly emerging as a strategic priority for businesses, governments and consumers around the world, and with its central role in societies, the financial sector is front and center in this drama.¹ But is the concern justified? Are the dangers real? Is the attention of time and resources necessary? Is the financial sector prepared to face whatever trouble is in store?

There are even deeper core issues for central banks: What are the supervisory and regulatory roles in this new frontier? How can supervisory and regulatory authorities control risk without inhibiting innovation? As the public trust in financial systems must be maintained while they undergo the digital revolution, can central banks avoid playing a leadership role?

The Asia-Pacific region is a major force in cyber matters, being a prolific supplier of Information and Communication Technology (ICT), the host of the world's largest netizen populations, and an increasingly important voice on international cyber security policy.² Thus cyber security matters are not foreign, but on the contrary, an indigenous subject for the region.

After establishing the need for central bank due diligence and leadership in regard to cyber security, this paper provides an introduction to key concepts that position strategies for mastery based on the right mindset and management approaches.

2. Background

The emerging electronic world offers a plethora of innovation and the chance to do things that prior generations only dreamed of. But aside from dreams, ICT's tangible impact is clear, evidenced by its high correlation with economic benefits for societies. The Internet is both a major component of Gross Domestic Product (GDP) for over 70 percent of global GDP and a major factor in GDP growth.³ The desires for e-government, e-commerce and e-banking are surging forward. The momentum for technology uptake has no end in sight. Yet inherent in this new environment are brand new hazards for stewards of civilization. We have welcomed relatively unfamiliar elements into our most intimate dealings. Artificial intelligence, pervasive connectivity and instantaneous transmissions are now part of our front and back offices, part of our peripheral and core operations and part of our public and most restricted communications. A downside of the use of these powerful means has been a rapid rise of e-theft, e-crime and e-fraud (see Insert A, page 38).

This paper submits that the financial sector, and in particular, its leading institutions such as central banks, must step up to face what are very real dangers of

reliance on ICT to financial stability. After establishing the need for due diligence for cyber security, the paper introduces the key elements of a mindset for mastering cyber security. Next, the current approaches are explored and contrasted with the key elements of a management system that is likewise designed for mastery. Finally, practical next steps are offered to build confidence in taking the first hard steps toward improving a cyber security mindset and management system, no matter where on the maturity curve an institution or economy may be. While this paper is not a vehicle for prescribing specific regulations, it does provide key characteristics of supervisory and regulatory approaches that will be most effective.

The following discussion does not repeat readily available, general information about cyber security. Rather it advances the discussion to those few defining issues that will ultimately determine excellence in managing financial stability. It is worth noting upfront that the guidance offered here challenges the mindset and management status quo of practitioners of even the most developed economies by identifying defects in common perspectives and practices. Thus this paper submits that the cyber frontier is indeed dangerous and concerns are justified, however it offers a new approach and higher benchmark for effective resource utilization.

3. Importance of Cyber Security Due Diligence

The financial sector is undergoing a profound electronic transformation. Even with this dramatic change, banking customers rely on financial institutions to protect their assets. This is inherent in the banker-customer relationship. The challenge to maintain that trust is higher than ever before, as a brief reflection on history portrays.

The path that economies have traversed from bartering with goods and services, to precious metals, to a self-defined currency, has now arrived at essentially *invisible* stored information as the means of transaction and record keeping. As it has been travelled in history, this course has required evermore trust along the way. The value of a lamb or day's labor was tangible to the buyer and seller in ways that precious metal was not, yet the convenience and portability of this innovation were a trade-off that history welcomed.⁴ The subsequent transition to a paper currency was a larger leap of trust; indeed some are still not comfortable with it. Yet this innovation similarly introduced multifarious benefits as its worldwide adoption gives evidence. Like the previous transformations, the present one ushers in a wide range of benefits that enable economies to thrive like never before. Farmers in remote villages struggling in underdeveloped economies use mobile smart phones to check true market value of chickens they bring to market; investors issue voice commands via their equally smart phones to buy and sell stock as they multitask; deal-clinching handshakes and smiles are facilitated by confirming real-time account transfers a half a world away; and central banks settle lifeline transactions with private institutions each day via computers, databases and software controlled algorithms. For each of these and the other countless scenarios, are numerous modes of failure that can devastate the trust of users: the market quote can be hacked and falsely presented, the trading platform can be manipulated with a bias,

an account could be compromised and liquidated and settlement systems can crash. While there are many participants in the sector that must contribute to securing ICT infrastructure, above all, due diligence by central banks in **preserving trust in the invisible electronic currency at the core** of the financial system is vital to financial stability.

The operations of banks and other regulated financial services providers have intense reliance on electronic data. Their investments in ICT are nontrivial as high quality data management and data analytics are critical prerequisites to prudent risk management and strategic and tactical decision-making. Banks' competencies in protecting the integrity of their information technology control environment and customer data security are critical to avoiding serious financial loss or reputational damage. Due diligence in preserving financial stability cannot be accomplished without due diligence in cyber security matters. The simple truth is that modern **banking is inseparable from ICT**. Accounting, transactions, trading, investments, interest calculations, lending, deposits, withdrawals, payments, clearing, settlements ... are all accomplished electronically. The requirement is *not* a diligence that can be delegated to "the IT room". On the contrary, board rooms must step up to increased awareness and responsibility for the stability, security, reliability, resilience and robustness of what is now the core fabric of their operations. As the author heard one Indian bank Chief Operating Officer (COO) observed, "we are really an IT company wearing the skin of a bank."

The Bank for International Settlement (BIS) Basel Committee on Banking Supervision introduced operational risk as an element of the first of its "Three Pillars" of sound banking practice. The Basel II Accord defines *operational risk* as "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events."⁵ In modern banking, "processes" are largely performed via electronic means. Likewise, "people" perform their various functions in a banking environment via electronic means. Even the banking "systems" are implemented by electronic means.

The inescapable conclusion is that due diligence in **cyber security is central to operational risk management**. Furthermore, "external events" can have a direct or indirect impact on financial stability via ICT. Examples of the financial sector being shocked by external events include the 2006 and 2009 severing of undersea cables in the Luzon Strait and the 2001 9-11 terrorist attack on New York City.

The due diligence of **central banks can have a positive influence** as they recognize and respond to cyber security issues, i.e. to their respective spheres of influence: private banks and other financial institutions.⁶ This influence follows from the general stature of the central banks as being the *conscience* of financial stability and thus an assumed role model, as well as from the unique functions of lender of last resort, supervisor and regulator, the exact combination of which depend on a given institution. Thus cyber security is a vital consideration for the three core objectives of central banking: monetary stability, financial stability and, safe, secure

and efficient payment and settlement systems. Payment and settlement systems rely on a flawless electronic transfer to ensure smooth functioning. Conversely, negligence in this area can have a negative impact and influence. As prioritized by the G20, the 2007-08 Global Financial Crisis (GFC) reform agendas of international regulatory standard-setters for the financial services industry have been primarily focused on more fundamental financial stability and prudential matters, such as the Basel III capital and liquidity standards. This prioritization has led to deferral of international policymakers' consideration of other important regulatory policy issues such as cyber security. As will be shown below, there are major aspects of the status quo in supervisory approaches regarding operational risk that can be improved.

The current situation can be further summarized as one where the banks are not homogeneous, generally operating with good management practices, dealing with the risks they are aware of, and implementing common practices that have limited effectiveness.⁷ Furthermore, ICT oversight commonly involves stakeholders, procedures, accountability, and other mechanisms of sound risk management. However, as a whole, the situation demands a closer strategic involvement from their boards to make sure the proper organizational attention and oversight are being pursued. While there are many priorities for oversight, cyber security is one that deals directly with reputation, which in turn deals with public confidence. Any time there is a crisis situation, there are two effects: (i) the actual loss, if any; and (ii) the potential longer term impact of public confidence, which can be reflected in numerous ways (e.g., customer turnover, reduced stock price). With cyber security, a single event can take but an instant but have long lasting damages.

Thus cyber security due diligence is important for central banks because (i) public trust in electronic currency at the core of the financial system is essential, (ii) banking is inseparable from ICT, (iii) operational risk management requires it, and (iv) leading institutions can have a positive influence on the financial system. Banks that manage cyber security effectively will satisfy customers, fulfill regulatory expectations, avoid costs of excessive exploitations, protect brand reputation, and maintain a competitive advantage. Management expert Peter Drucker taught that "Management is doing things right; leadership is doing the right things."⁸ Now that we have established that cyber security due diligence is "doing the right thing", we next turn to "doing things right", first by considering the right mindset.

4. Mindset for Mastering Cyber Security

Having a right mindset is the first step in being prepared for managing cyber security. There are several key concepts, which if acknowledged at the onset, have a long-term benefit for managing cyber security effectively. These concepts, each of which is a corollary to a hazard to be cautioned against, are worth covering deliberately here because, though they may seem quite obvious, are actually commonly overlooked, or otherwise not perceived with much clarity. The landscape of internal and external ICT infrastructure that routine banking relies on is highly complex and continuously

evolving. These concepts are reference points to assist navigating that complexity and evolution. Once grasped these concepts can serve as a trusted touchstone when considering options for managing cyber security. Surprisingly, each of these concepts is often missed by practitioners in even the most developed institutions and economies; thus their value is useful throughout the full range of the cyber security management maturity curve.

4.1 A Mindset to Achieve Control

Classical quality control principles, which in the past century have transformed the productivity and quality across the complete spectrum of sectors around the developed world, have not yet been applied well to cyber security. One of the key principles of modern quality management is seeking and establishing controls that can accomplish performance improvements when needed.

Caution 1: Reactive Management Fosters Instability

We begin with a big picture of the major trend dynamics across the ICT landscape, namely, technology (T), technology adoption (A), criminal exploitation of technology (X) and management of technology risk (M). Management here refers to the development and implementation of policies and practices to ensure uncompromised assets and services. Figure 1 illustrates the relationship between these trends relative to each other and their respective rates of advancement over time.⁹ Amongst these four trends, there are six potential inter-relationships. The sequencing of these trends is as follows:

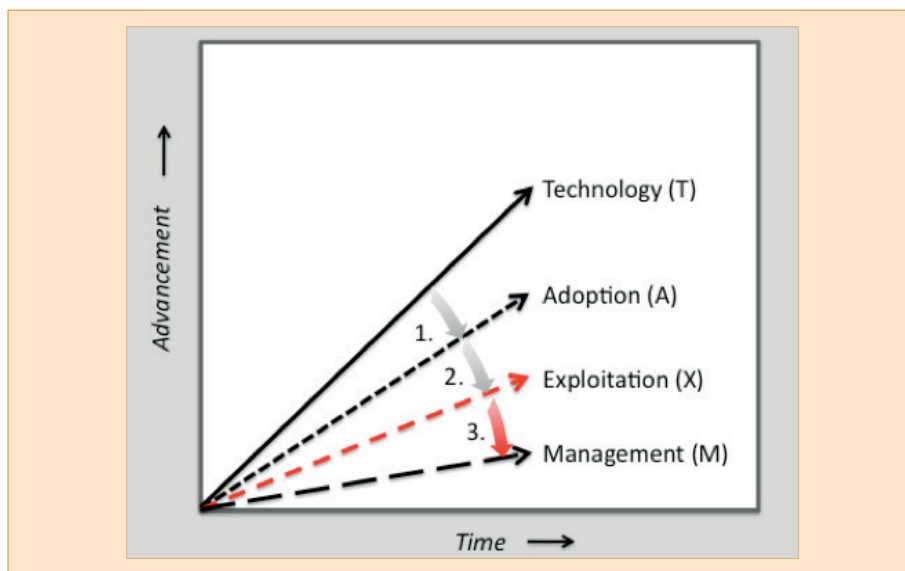
1. Technology drives technology adoption [T → A]
2. Technology adoption enables criminal exploitation [A → X]
3. Management responds to the criminal exploitation [X → M]

The third relationship is what is fundamentally problematic with the big picture. The reactive posture of key management activities enables cyber crime to thrive.¹⁰ The primary reason why management (M) is presently lagging and has the slowest rate should be obvious. The primary impetus for management (M) as routinely practiced in government and industry is the need to react to a problem, in this case criminal exploitation (X).

There are 3 major concerns with this orientation. First, it is costly, as reacting to a growing problem is rarely an efficient strategy. Second, it is unstable, because malicious actors are only making use of a subset of the full set of possible exploitations at any given point in time. The complement of remaining exploitations can at any time be discovered and exercised and further deteriorate the integrity of a financial system or institution. Third, it propagates a less desirable philosophy and balance of core competencies, both within an institution and amongst the external resources that are positioned to assist the institution. While rapid response skills will always be needed,

the preponderance of such when there are limited resources results in an undesirable trade-off that gives up more leveragable competencies such as proactively deployed science, technology, engineering and mathematics (STEM). Loading up on a reactive posture is *not* a winning mindset when the number of sources and the number of types of threats are growing faster than your own capabilities in an environment of pervasive global connectivity.

Figure 1. Dynamics of the ICT Infrastructure Landscape with Reactive Management



The first and second relationships cannot be altered, i.e., adopting technology requires it to exist, and exploiting technology requires it to be deployed. However, the third relationship can be turned. This opportunity is picked up next in the discussion and presented as the corollary to Caution 1, along with the remaining three inter-relationships, i.e. technology and management [T&M], technology and exploitation [T&X] and adoption and management [A&M]. These three relationships are neglected in the reactive management paradigm.

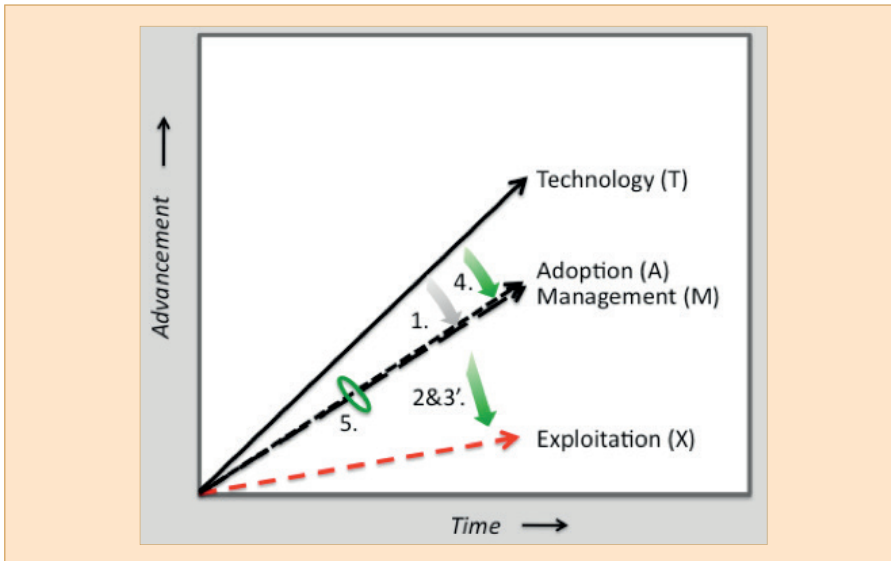
Concept 1: Coordinate Technology Adoption with Technology-Informed Management

In a mindset prepared for mastering cyber security, still at the forefront is the fact that technology (T) drives technology adoption (A). However, the following relationships are now significant (Figure 2):¹¹

- 4. Management is informed of Technology [T → M]
- 5. Technology Adoption and Management Are Coordinated [A ↔ M]
- 2&3'. Coordinated Technology Adoption and Management Impede Exploitation [(A ↔ M) → X]

The drive to achieve control positions management planning and resource application earlier in the technology deployment lifecycle. This is enhanced with intelligence regarding the technology.¹²

Figure 2. Dynamics of the ICT Infrastructure Landscape with Proactive Management



4.2 A Mindset that Acknowledges Strengths and Weaknesses

Since it is well established that the use of ICT in banking is not going away, there are some *unfriendly* trends from a cyber security management perspective, that must be lived with. Once we accept these hard realities, we can use their constraints to concentrate available rigor effectively in the solution space.

*Caution 2: Connectivity, Complexity and Criticality*¹³

The recent **connectivity** accomplished by the Internet thus far, though breathtaking, is not plateauing, but rather on the verge of an explosion far greater than what we have seen to date. The Internet Protocol Version 4 (IPv4) allows for approximately 4.3 billion unique addresses.¹⁴ This current address architecture provides approximately enough addresses for each person on the planet (~7 billion), but not enough. Responding to this address exhaustion, and anticipating the Internet of Things (IoT), IPv6 is now being deployed at various stages around the world. IPv6 provides an astronomical number of unique addresses (hundreds of undecillions); if there were one thousand more people on the planet, *each* could have *one trillion times one trillion* unique addresses on the Internet!¹⁵ Why so many addresses? Electrical engineers and other stewards of the Internet's future envision that anything deemed important will be networked: vehicles, appliances, cattle,

nanotechnology in bloodstreams, etc., thus is the future IoT. Each “thing” will thus potentially be connected to banks and other financial institutions, with the possibility for all sorts of creative billing and financing models, which leads us to the next foreboding trend.

The *complexity* of the Internet is overwhelming. Presently, the number of potential interacting pairs of endpoints on the Internet with IPv4 is referred to as *quintillions* (a number with 18 zeros after it); this number grows to *trillions of vigintillions* (76 zeros after it) with IPv6.¹⁶ Moreover these numbers just represent the potential connecting entities – the complexity is still vastly greater as it will involve much anticipated elaborate interactions. So the explosion of connectivity, is even further “outnumbered” by the trend of complexity, which is further impelled by such features as open platform architectures that enable user-generated applications, reliance on artificial intelligence to make decisions from complex “big data” analysis, interactions among machines that are empowered to manage the background tasks of our lives (including finances) and new business models that integrate real-time information from sensors, inventories and market supply and demand like never before.¹⁷ Intelligent, networked technology will be a decisive enabler as competitive edges are defined by the ability to make decisions a split second faster than a competitor. Already, the new informed capabilities are being dubbed “smart grid”, “smart living”, “smart healthcare”, “smart weapon”, “smart government”, “smart banking”, etc. The advantages of “being smart” will increasingly drive reliance on advanced ICT for everything that is important, which leads us to the next disruptive trend.

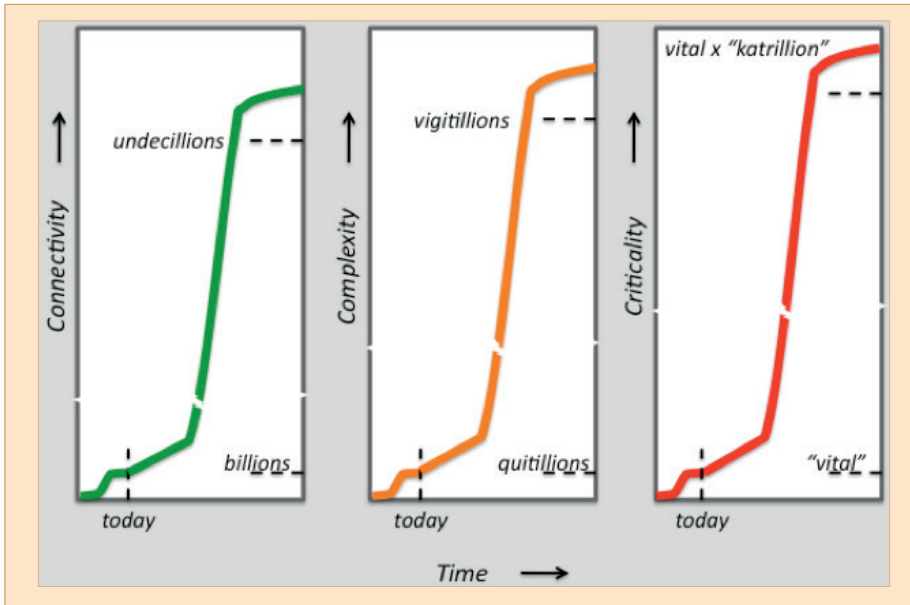
In light of the above, consumers are poised to continue demanding convenient delivery channels for banking services that may introduce new material risk factors. Banks’ financial soundness depend on their ability to understand and manage such risks to maintain consumer confidence and a favorable reputation.

The supply chain for ICT is still another aspect of the complexity trend, as the software, systems and services relied upon are delivered by an intricate web of interdependencies that crisscross the globe.

There is coming a need for important things to be done faster, better and cheaper. Advanced ICT offers this. Thus the third unstoppable trend is for *criticality* to be ever increasing; i.e. ICT must to be more secure and more reliable because we are counting on it more today than yesterday.

Summing up the above, it is evident that the practice of cyber security due diligence will only become much harder as connectivity, complexity and criticality skyrocket. Given its central role, the banking industry cannot avoid the hard realities of these trends. Furthermore, there is no solution presently employed to counteract the difficulties presented by these trends (Figure 3).

Figure 3. Unstoppable Trends of Connectivity, Complexity and Criticality



Concept 2: Solution Space of the Asymmetric and Finite

Given how there are unstoppable long-term trends making cyber security due diligence more difficult, and that there are no solutions being widely deployed to neutralize the challenges of any one of these trends, a calm mindset is needed that will be deliberate in identifying fulcrums on which to leverage an advantage. Economical solutions will need to be orthogonal to the massive dimensions described above, in order to avoid costs that also follow the explosive growth rates. Thus possible attributes of the solution space that can survive this harsh arena are those that can add significant value in ways that are asymmetrical to the overwhelming tsunami of connectivity and complexity underway. Viable paths forward will be those that find insights akin to scientific constants that are not tracing the exponential curves, but rather have a finite nature. Winning strategies will thus have a mindset that recognizes innovation leveraging the asymmetric and the finite.

4.3 A Mindset for Completeness and Accuracy

As one of the few areas with growing budgets, there are no lack of cyber security products and services on the market.¹⁸ In addition to the private sector, governments have likewise prioritized cyber security as an issue to be addressed, putting forth high level policy statements and initiatives, which often cite the importance of the issue for national economic interests.¹⁹ Meanwhile, the financial sector has several initiatives underway that include guidance for cyber security assessments or other checklists and best practices. One notable example is Canada’s Office of the Superintendent of Financial Institutions 2013 publication of a cyber security self-assessment.²⁰ Delving

into all of these outputs, one gets the sense that the efforts are at a relatively early stage, coming short of mastery. The language and descriptions lack the earmarks of performance benchmarks and expectations for certain control of the situation when investments of resources are made. As an aggregate, these outputs also both reflect a high respect for cyberspace as a medium and convey a sense of mystery as to its nature, combining to reveal a lack of confidence that completeness and accuracy can be achieved.

Caution 3: Abstractions Are Deceptive

In technology, as in other fields like economics, it is often beneficial to make use of simplifications of a complex subject in order to convey a particular point. In this regard, analogy, patterns, and models are useful in enabling efficient knowledge transfer. There are many instances in the practice of cyber security where abstractions are utilized. These include protocol standards that define the acceptable inventory for given fields, threat modeling that anticipate the interests of a hacker, or statistical risk analyses based on historic events, to name a few. These abstractions are often very useful, and even necessary at times. However, a miscalculation is made when the abstraction is believed to be the same as reality. The basic limitation with nearly all abstractions is that they are at best a shadow of reality, and at worse, they can convey inaccurate aspects of reality.

Variations from Plan Are Inevitable

One common misfortune is when one relies upon an abstraction that is based on how things are *supposed* to work (e.g., a protocol specification). In other words, things may work perfectly on paper and according to plan, but what is happening on paper is not what is happening “on the ground.” History is ripe with such examples of a failure to adequately anticipate variance. One example that lies at the roots of modern cyber security is the German Enigma machine, which enabled secure communications in World War II. The Germans were convinced that the Enigma’s advanced encryption was uncrackable. No one would have the time or mathematical ability to work through all possible combinations that it could generate when coding a message. The way it was *supposed* to work per plan, maybe so. However, operators of the typewriter-like boxes did not always follow procedures, being either forgetful or lazy. This variance, when combined with another oversight, led to the big break for hacking into the Enigma. The other insight came to Allied code breakers when they recognized that daily weather forecast broadcasts from German U-boats in the North Atlantic followed a consistent format. The variation of actual from intended use led to a compromise of the security of Germany’s most sensitive communications. In this case, the failure had a positive benefit of bringing an earlier end to the war.

Historic Analogies Are Limited

A second common shortcoming of abstractions is that they can be overly reliant on experience. Experience being so valuable, it must not be discounted. However,

the caution here is to *not inflate* its value, such that it is esteemed as being a sufficient intellectual basis for preparedness for the future. The common disclosure made to personal investors comes to mind: “past performance is not indicative of future performance.” This axiom applies well to cyber security, as there are new permutations of attacks, literally, every day. Though not a cyber-related example, given that its features have been so studied, it is worth considering here a more recent example from history: the September 11, 2001 terrorist attacks on New York City. Prior to these attacks, expressed concerns about unsecured cockpit doors did not resonate with the model for evaluating risk. Why? The threat model for airplane hijacking prior to 9-11 did not account for the latent vulnerability of cockpit door access and a willingness of hijackers to sacrifice their lives for the mission. No one had tried this before, so the threat model missed it. The threat-oriented perspective dominates much of the cyber security industry. There are countless companies that provide ever-faster capabilities to learn about the latest threats and incrementally react better to them. It is very important for a cyber security strategy to make use of such experience and historic knowledge, but it is not enough because it can be assumed that there are always latent failure modes, as Concept 3 will further assert below.

Extensions Beyond Usefulness Cause Error

A third problem with abstractions is that they can just plain convey a fallacious notion. This is probably seldom the intent, but rather a collateral or derivative effect. A present day example is the popular term “cloud”, which refers to distributed processing and data storage across networks that can span a region or even the world. Since the mid-1980s network engineers drew cartoonish clouds on whiteboards when they were in a situation where they did not want to elaborate on the details of a network, but rather wanted the focus of attention to the systems or devices on the network peripheral. It was convenient; in this context no harm was done. However, the use of a cloud for simplification has turned the term into a buzz word of ICT market-wide (i.e. worldwide) proportions!

A few years ago while attending a major international cyber security conference in Beijing, the author heard the Chief Technology Officer (CTO) of a popular Internet company make a 30-minute presentation on “the cloud” that was based on the principles of different types of real clouds (e.g., cirrus, stratus, cumulonimbus). It was interesting, but had no basis in reality. Distributed computing and processing is *not* a cloud, *nor like* a cloud. Other than the initial simplification on the whiteboard, the parallels are not beneficial. The concern is not based on a single speech; sadly, but far from it. Far too few stakeholders, whether they are individual customers or the managers of large financial institutions, really understand what is happening when they rely upon a “cloud” service. A Silicon Valley-based survey found there is gross ignorance about what the so-called cloud is, even in the most developed societies, and even amongst those that are using “cloud-based” services for banking.²¹ Given the priority of maintaining trust for financial stability, vast gaps in understanding like this are a public relations crisis waiting to happen. Due diligence, at least in the financial services sector, should not allow conversations to remain at the “cloud” level. Banks need insights into the inside of

these clouds, assurance of diverse physical routes, geographically-acceptable data storage locations, access control practices, redundancy, etc.

In review of the above, abstractions have useful function but at some point must be seen as a crutch to be abandoned. Understanding these limits is crucial to avoiding major oversights that, if exploited, could lead to compromise of financial ICT systems or services. When the stakes are high, as they are for the financial stability of an economy, operational risk management should be based on the tightest possible understanding of reality, even if new training and extensive rigor are required.

Concept 3: Reality-based Framework is Essential

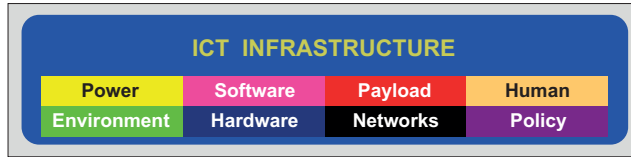
The need for a sound and effective framework is introduced in the Basel “Core Principles for Effective Banking Supervision”, which articulates an Operational Risk, Principle 25, as follows:

“The supervisor determines that banks have an adequate operational risk management framework that takes into account their risk appetite, risk profile and market and macroeconomic conditions. This includes prudent policies and processes to identify, assess, evaluate, monitor, report and control or mitigate operational risk on a timely basis.”²²

Working from a foundation tightly coupled with reality is essential, making it possible to most effectively “identify, assess, evaluate, monitor, report and control or mitigate” cyber security risk. But how can a leader of financial institutions, whose primary expertise is not science, engineering or technology, accommodate such a need? How can this be practically achieved on a broad scale?

This concept does require a commitment by the most affected to learn new things; this is unavoidable. The key is that asymmetric approaches for grasping the core set of principles are available, thus making the task practicable. One framework that has been proven to be both accurate as a reflection of reality and effective in supporting proactive management of cyber security is the Eight Ingredient (8i) Framework (Figure 4). Its basic assertion is that cyberspace, or ICT infrastructure, consists of eight ingredients: environment, power, hardware, software, network, payload, human and policy (or more completely: Agreements, Standards, Policies and Regulations –ASPR) (Insert B).²³ Any seven ingredients would be too few, and a ninth is not needed. The 8i Framework is crucial in that its ingredient approach is asymmetric to the big trends, meaning it does not change, despite the exploding numbers. The 8i Framework is also accurate relative to reality, meaning that it avoids the pitfalls of abstractions discussed above, by not overextending itself beyond its range of accuracy, remaining grounded in the simple reality that cyber space has a finite number of distinct ingredients. The 8i Framework also brings completeness with its constant eight ingredients, which hold not only for the previous century of electronic communications but also for the foreseeable future.²⁴

Figure 4. Eight Ingredient (8i) Framework



The more convinced a mindset is of the need for the strictest possible alignment with reality, the stronger it is positioned to master cyber security and avoid excessive risk. The next set of benefits that can be derived from this approach is that each of the eight ingredients has a finite set of intrinsic vulnerabilities.²⁵ This is significant because the only way that a threat can have a negative impact is to exercise one of the intrinsic vulnerabilities, of which there are on the order of one hundred, a very manageable quantity. The means by which the most common forms of cyber security threats do harm can be shown to be associated with one or more of the intrinsic vulnerabilities of the eight ingredients (Insert A). Furthermore, it could be stated that *all* systemic risk related to ICT is tied to one or more of the finite set of intrinsic vulnerabilities. The unwelcome news is that with cyberspace there are *new* risks for the financial sector originating from these intrinsic vulnerabilities. Further, none of these intrinsic vulnerabilities can be completely removed – they are always there. The good news is that there is a finite set of intrinsic vulnerabilities and thus the overwhelming complexity of cyberspace now has a handle from which we can get a firm grip.

Like other dimensions of risk management, ICT risk is often considered in a cost-benefit context. One of the implications of this consideration is the extent to which some functions may be outsourced. For example, a smaller bank may find developing the same internal capabilities as a large bank to be cost prohibitive. In light of this, central banks supervisory and regulatory measures should anticipate the need for flexibility in implementing the above concepts into due diligence strategies.













One unifying theme of this paper is that financial institution leaders must take more responsibility and accountability. Securing ICT systems and services is the business, the mission and the job of a financial institution in the modern world. Fortunately, there are cautions and key concepts that can serve a leader well in making rapid progress on the cyber security management curve.


Like other dimensions of risk management, ICT risk is often considered in a cost-benefit context. One of the implications of this consideration is the extent to which some functions may be outsourced. For example, a smaller bank may find developing the same internal capabilities as a large bank to be cost prohibitive. In light of this, the central bank’s supervisory and regulatory measures should anticipate the need for flexibility in implementing the above concepts into due diligence strategies.









Insert A. Examples of Cyber Security Threats Financial Services Institutions Face
 (for their operations or for their customers' use of their services)

Threat	Description	Ingredients with Intrinsic Vulnerabilities Exercised
Account Aggregation	Consolidation of multiple online financial accounts from banks, billers, brokerages, etc. providing a “one-stop” site (increases consequences of a compromise)	
ATP	Advanced persistent threats involve coordinating multiple methods of identifying and exploiting a target's vulnerabilities over an extended period to do harm	
Backdoor	A method of avoiding detection while bypassing normal authentication for accessing a system	
Bloatware	Accumulation of unused software programs that remain after de-installation and become a risk for exploitation	
Botnet	Collection of networked programs communicating with each other in order to perform tasks	
Browser Hijacking	Unauthorized modification or control of a web browser's settings	
Cryptoviral Extortion	The use of public-key encryption technology to encrypt a user's data and withhold the session key until a condition is met (e.g., payment)	
Data Breach	Unauthorized access to restricted-access data	
DDoS	A distributed denial of service attack makes use of the capacity limitation of an enterprise network ingress with extreme traffic loads	
Defacement	A hack on a website that changes its appearance or content	
Drive-by-Download	Software functionality that is loaded onto a user's device, without their knowledge intentionally	

Threat	Description	Ingredients with Intrinsic Vulnerabilities Exercised
Hacking	Gaining access to an asset in cyberspace without the presumed required knowledge or official credentials	
Identity Theft	The use of another's identity in cyberspace	
Imposter Applications	An application placed in an app store that masquerades as a commercial application	
Insider Threat	A person inside an organization with access to ICT whose conflicting interests are poised to harm the organization	
Keyloggers	Recording the keystrokes of a device in a covert manner	
Kleptography	The practice of stealing information without being detected	
Malware	(Malicious software) software code that is intended to do harm	
MITM	Man-in-the-Middle is active eavesdropping where the unauthorized party is inserted between sender and receiver and can emulate traffic coming from either direction	
MITMO	Man-in-the-Mobile compromise allows unauthorized party to control a mobile device and communications (i.e. texting) to and from it without the user's knowledge	
Phishing	Use of electronic communications to masquerade with trusted identity to capture sensitive information	
Ransom-ware	Software that takes unauthorized control of a device, or some part of it (i.e. data), until a payment made, or some other condition is met	
Rogue Application	Software program that misleads end users to believe that it is a well-known or otherwise safe application	
Rooting	Gaining privileged control (root access) on an operating system	

Threat	Description	Ingredients with Intrinsic Vulnerabilities Exercised
Rootkit	Software designed to hide the existence of certain processes or programs from normal methods of detection and enable continued privileged access to a computer	
Smishing	(SMS phishing) the use of mobile phone text messaging to trick user into providing sensitive information	
Sockpuppet	A false online identity	
Spam	electronic messages in any form that are widely distributed in high volume and are uninvited by the recipient; often the vehicle of malicious code	
Spoofing	An electronic communication with a forged sender address	
Spyware	Software that is running on a device unbeknownst to its user to gather information	
SQL Injection	A code injection technique where malicious Structured Query Language are populated into an entry field for execution	
Steganography	The practice of using hiding information within a larger profile of information, such as an image	
Trojan	Software that contains concealed functionality	
Virus	Software code that attaches itself to software programs, replicates itself and spreads to infect other files or programs	
Vishing	Use of voice communications to trick an individual to give up personal or financial information	
Worm	A standalone malware computer program that replicates itself in order to spread to other computers	

Threat	Description	Ingredients with Intrinsic Vulnerabilities Exercised
Zero-Day	A threat that exploits a vulnerability in a software program prior its developers having a chance to implement a patch for the software	

Key to Ingredient whose Intrinsic Vulnerabilities are Exercised			
 Environment	 Software	 Payload	 Human
 Power	 Hardware	 Network	 ASPR

5. Management for Mastering Cyber Security

The previous section emphasized three areas of consideration for creating a mindset to master cyber security. This is the beginning of a journey, the departure point. There is of course much more that must be done. The discussion now briefly turns to additional strategic suggestions for managing with due diligence.

Senior Leadership

Financial stability is now vitally reliant upon due diligence throughout the ranks of financial institutions. Indeed the trustworthiness of the financial institution is inseparable from the trust in the integrity of the institution’s computers, online services and electronic data. Thus, no less than the heart of financial stability, the public trust, is at stake when cyber security strategies are designed, cyber security policies are deployed and cyber security vigilance is pursued. Such criticality requires the most senior management of banks to be actively engaged in ensuring cyber security due diligence.

Best Practices

Best practices are a highly preferred method of knowledge transfer when dealing with fast advancing technology due to the speed with which they can be developed; i.e. relative to regulation and standards, which take much longer (Figures 1 and 2). A key to managing best practices development is to focus on addressing the intrinsic vulnerabilities, independent of specific threat knowledge. This concept may seem subtle when it is first read, but its effect when guiding a security strategy is profound. The tangible benefits are reduced cost, higher performance and a foundation for achieving control. Best practices strategies should include both countermeasures for preventing the exercise of an intrinsic vulnerability as well as ameliorate the impact should prevention fail.

Holistic Picture

All causes of harmful events need to be considered, without bias. It follows when focusing on intrinsic vulnerabilities, as opposed to threats, that the intent (or lack of an animated intent) is less relevant than the need to avoid a compromise. Operational risk should be objective, avoiding bias toward prioritizing malicious acts, relative to unintentional or natural disaster-caused events. However it is a seemingly universal preoccupation to pay much more attention to malicious acts relative to natural disasters.

“I am not angry - except perhaps for a moment before I come to my senses - with a man who trips me by accident; I am angry with a man who tries to trip me up even if he does not succeed. Yet the first has hurt me and the second has not.”²⁶

This is a common experience and demonstrates our preoccupation with malicious human threats in a way that is not related proportionally with risk or impact. To date, by far, most disruptions in service occurred from unintentional events.²⁷

Performance Measurement

It is most essential to measure what matters, not what is most convenient. This sometimes is in contrast to the common practice of measuring conformance to industry common practices. The ultimate evaluation of the effectiveness of a cyber security program should be based on the actual performance (i.e. counting actual compromises) relative to benchmarks.²⁸

Because actual events may (fortunately) still be rare events, their statistical frequency may be rare. It is therefore important that oversight boards not overreact to a single event based on its visibility, but rather make judgments based on a sound understanding of the statistical variability associated with such performance statistics.

Select Partners Wisely

With cyber security becoming a growing market, there are many companies eager to offer their products and services. Just an observation of the number of new companies emerging in the industry over such a short period of time makes the depth of expertise questionable across the aggregate. It is important to select partners who share a mindset to mastery, making it smaller, even though such a strategy is counter to the business interest of firms whose revenue generation is directly correlated with a thriving cyber security problem.

Developing Economies

Developing economies are of special concern as they are consistently targeted by malicious actors to be used to set up botnets and otherwise become the sources of attacks.²⁹

Developing economies should also be cautious of uncritically following the examples of developed economies with the assumption that their practices represent the soundest approaches. On the contrary, with their limited resources, developing economies must be strict in their disciplined use of existing resources, not having the luxury to lose money to strategies that are reactionary, overextending an abstraction or otherwise limited in effectiveness.

Regional Initiative

In cyberspace there are no national borders. With this in mind, it has been said, “we are all in this together” and “we are only as strong as our weakest link”. It thus follows that international cooperation can be quite beneficial to all involved. The benefits of such cooperation include increased awareness of trends, more effective best practices, coordination in solving cross-border issues, and other efficiencies related to progress on the maturity curve of mastering cyber security due diligence. A practical first step toward reaping these benefits is to begin with regional-level collaboration. With the overarching aim to improve the security of stability of ICT infrastructure in the Asia-Pacific region, central bank leaders are encouraged to consider both problems and solutions that they can bring to such a discussion and take advantage of opportunities to engage with their peers. The anticipated important output of such collaboration includes harmonious supervisory and regulatory policy frameworks with regards to cyber security due diligence, which does well to serve the public good and confidence in the stability of the region’s financial systems.

In summary, the banking community must answer the question “how should this cyber security challenge be met?” It is tempting to answer this question with a description of how the challenge *is currently* being met. But that is a different answer than how it *should* be met. Both responses have been explored throughout this paper. It is the general consensus by experts that the bad actors are winning up to this point.³⁰ There are ample demonstrations via frequent media reports of embarrassing breaches of financial records across a wide range of commercial entities. It is thus quite evident that the malicious actors who are on the offense have enjoyed the advantage despite all that is commonly deployed to date. It is time to turn the tables.

Insert B. Ingredients, Intrinsic Vulnerabilities & Events
(Examples)

Ingredient	Description	Intrinsic Vulnerability*	Historic Event
Environment	Physical location of ingredients	Accessibility	Unauthorized device installed in Barclays internal network (2013) ³¹
Power	Electrical supply for hardware and environment	Loss of potential	Northern India power blackout precedes central bank cutting growth outlook by 11 percent (2012) ³²
Software	Programs providing functionality	Accessibility	U.S. Federal Reserve web site loses control of web site to hacktivists (2012) ³³
Hardware	Cables, semiconductor chips, electronics	Susceptibility to physical damage	Undersea cable cuts cause catastrophic shock Hong Kong financial systems (2006, 2009)
Payload	Information transported on infrastructure	Emulation	ANZ Bank in Vietnam is one of many banks whose customers received phishing emails (ongoing) ³⁴
Network	Configuration of nodes and their interconnection	Capacity limits	Targeted DDoS attacks on U.S. banks (2012-2013) ³⁵
Human	Involvement in entire ICT lifecycle	Cognitive – ability to be deceived	Fiji students open fake accounts with information obtained from social networking sites (2014) ³⁶
ASPR (Policy)	Inter-entity arrangements enabling behavior anticipation	Predictable behavior due to ASPR	A Man-in-the-Middle insertion enables unauthorized transfers from a Philippines bank account (2012) ³⁷

* In these examples there is often more than one intrinsic vulnerability exercised by the threat; e.g. the Payload example also involves the Human intrinsic vulnerability of cognition, i.e. being able to be deceived.

6. Conclusion

The previous pages reviewed compelling motivations for the financial services sector, and especially leading institutions like central banks, to be resolved in their commitment for cyber security due diligence. Reasons were established for why this effort is needed now, without delay. The limiting characteristics of current approaches were contrasted with the optimum approach in the context of a mindset and management for mastery. For a starting mindset, cautions and corresponding corollaries were offered for three areas, namely: a mindset for control, for discernment of strengths and weaknesses and for completeness and accuracy. How should we then proceed?

The biggest themes of this paper are that (a) we must accept the fact that cyber security is here to stay as a growing challenge, (b) the current methods are having insufficient results, (c) central banks play a central role in preserving financial stability for their sector and respective national economies, and (d) having a strategic mindset is vital to give commercial banks the best opportunity to convert their limited resources into the best results in a sustainable fashion.

Notice

In regard to the actions called for this article, leaders of central banks and other financial authorities of the Asia-Pacific region will convene to discuss regulatory expectations with respect to banking cyber security risk controls at the:

SEACEN Cyber Security Summit 2014
“Demystifying Cyber Risks: Evolving Regulatory Expectations”
25-26 August 2014

Sasana Kijang, Bank Negara Malaysia
Kuala Lumpur, Malaysia

For more information, please contact: enquiries@seacen.org

Acknowledgement

The author expresses gratitude here to Stephen Malphrus (ret.) and Wayne Pacine of the U.S. Federal Reserve for their valuable insights through years of tutelage in previous collaborations.

* **Karl Frederick Rauscher** is the first Ambassador & Chief Architect of Cyberspace Policy of the Institute of Electrical and Electronics Engineers (IEEE), and serves as a Commissioner of the G8-initiated Global Information Infrastructure Commission (GIIC), and is in an advisor to senior leaders, including for the financial services sector, on five continents. He has served as CTO and Distinguished Fellow of the EastWest Institute and has facilitated the development of over 1,000 world-class best practices for reliable and secure communications systems, networks and services. He is a lifetime Bell Labs Fellow, cited for achieving the first “6 9’s” (99.9999% availability) for a real-time network system, and has 50 patents/pending. In 2013, *The New York Times* editorial board cited his guidance for China-U.S. bilateral cybersecurity cooperation in *Fighting Spam to Build Trust* as recommended reading for President Obama and President Xi.

Endnotes

1. The global cyber security market is estimated at \$77 billion in 2013 and projected to grow to \$120 billion by 2017. "Cyber-Security Market (2012-2017)," marketsandmarkets.com, Retrieved: 31 March 2014.
2. China's Huawei is the largest communications equipment supplier in the world ("Who's afraid of Huawei?" *The Economist*, 3 August 2012, Retrieved: 3 August 2012). India is similarly one of the world's largest producers of software. China has the largest number of mobile phone users (1.3+ billion) and Internet users (600+ million); India has the second largest number of mobile phone users (1.1+ billion) and third largest number of Internet users (150+ million); other countries in the top 20 of either category include Bangladesh, Indonesia, Japan, Philippines, South Korea, Thailand and Vietnam.
3. Estimates of 3.4 percent of GDP, and 10 to 20 percent of growth, Per: Manyika, James and Roxburgh, Charles, (2011), "The Great Transformer: The Impact of the Internet on Economic Growth and Prosperity," McKinsey Global Institute.
4. Bartering required a coincidence of wants.
5. Basel II: Revised international capital framework.
6. The term "central bank" used here and throughout to include alternative designations of "reserve bank" or "monetary authority."
7. Common practices include a focus on confidentiality, integrity and availability (CIA); applying a defense-in-depth strategy that involves layers (physical, network, operating system & application layers) of ICT systems; continuous monitoring and the use of automated tools (e.g., firewalls, intrusion prevention systems, anti-spam & anti-malware filtering); and an incident response team. More advanced organizations are also proactively engaged in cyber security collaboration with the critical infrastructure they rely upon (energy, communications, government, etc.) and periodic exercises.
8. Drucker, Peter F., (2003), "The Essential Drucker: The Best of Sixty Years of Peter Drucker's Essential Writings on Management," Collins Business.
9. The introduction of the relative comparison of advancement was first introduced in a presentation to the 2010 FIRST Technical Colloquium, Beijing, "The Rise of the 8th Ingredient- the Imperative of Addressing the International Policy Gap in Cyberspace."

10. While the author is very much aware that institutions have in place many proactive practices in their design and operation of ICT for security and reliability, the predominant posture across the financial and other critical sectors is one of reaction to the latest threats being presented.
11. Note that the sixth relationship, not discussed yet involves technology and exploitation (X). While malicious actors certainly have the opportunity to be earlier learners of emerging technology, and do make use of the opportunity, they do not have the controls of adoption and therefore this relationship [T&X] falls behind a coordinated adoption and management [A&M] capability.
12. The cost of perfect policy may not be desirable from a cost-benefit analysis, i.e. the cost of a minimal amount of loss due to criminal exploitation may be more tolerable than the price of achieving the ideal policy. The cost would include not only the direct expense associated with policy development but also the cost of delayed deployment of technology in a competitive environment.
13. The author credits Phil Reitingner with this alliteration for these three concepts.
14. $2^{32} = 4,294,967,296$ based on using a 32-bit (4-byte) address scheme.
15. $2^{128} = 340,282,366,920,938,463,463,374,607,431,768,211,456$ based on using a 128-bit (16-byte) address scheme.
16. Using the formula: $[n(n-1)]/2$, for IPv4: $[2^{32}(2^{32}-1)]/2 \sim 9.2 \times 10^{18}$; for IPv6: $[2^{128}(2^{128}-1)]/2 \sim 5.8 \times 10^{76}$.
17. The number of apps for both the Android and Apple devices is on the order of magnitude of one million.
18. Billed as the world's largest annual cyber security conference, the RSA draws a growing number of suppliers of products and services. The RSA 2014 exhibit hall featured approximately 150 vendors appealing to tens of thousands of security practitioners.
19. Examples include the 2014 Chinese government announcement of a new Central Internet Security and Informatization Leading Group to be led by President Xi, the 2013 European Commission "Cybersecurity Plan to Protect Open Internet and Online Freedom and Opportunity", the 2013 "U.S. President Executive Order - Improving Critical Infrastructure Cybersecurity"; India's 2013 proposed "National Cyber Security Policy."

20. Office of the Superintendent of Financial Institutions Canada, (2013), “Annex - Cyber Security Self-Assessment Guidance,” The Financial Service Roundtable (FSR) is a U.S. private sector organization that provides information for its members (see www.bits.org/publications/home/BITSProjects.pdf), Retrieved: 31 March 2014.
21. Half of Americans (51 percent) believe that stormy weather interferes with cloud computing. When asked what “the cloud” is, a majority responded it’s either an actual cloud (specifically a “fluffy white thing”), the sky or something related to the weather (29 percent). A majority of Americans (54 percent) claim to never use cloud computing. However, 95 percent of this group actually does use the cloud. Specifically, 65 percent bank online, 63 percent shop online, 58 percent use social networking sites such as Facebook or Twitter. Frank Packer and Haibin Zhu, (2012), “Most Americans Confused by Cloud Computing According to National Survey,” Wakefield Research, August.
22. Basel Committee on Banking Supervision, (2012), “Core Principles for Effective Banking Supervision,” Bank for International Settlement.
23. Rauscher, Karl. F., (2004), “Protecting Communications Infrastructure,” Bell Labs Technical Journal Homeland Security Special Issue, Volume 9, Number 2.
24. If a technology would be introduced that integrated an additional ingredient, it could be easily included in the framework.
25. Rauscher, Karl. F., (2004), “Protecting Communications Infrastructure,” Bell Labs Technical Journal Homeland Security Special Issue, Volume 9, Number 2.
26. Lewis, C.S., (1952), “Mere Christianity,” Book 1 Right and Wrong as a Key to the Meaning of the Universe.
27. Network Reliability Steering Committee (NRSC) Annual Reports, www.atis.org.
28. Rauscher, Karl Frederick and Erin Nealy Cox, (2013), “Measuring the Cybersecurity Problem,” EastWest Institute.
29. Examples of such targeting includes Africa, India, and Eastern Europe.
30. Menn Joseph, (2014), “Hackers Winning Security War: Executives,” Reuters, San Francisco, 2 March.
31. Dixon, Hayley, (2013), “Barclays Hacking Attack Gang Stole £1.3 Million, Police Say,” The Telegraph, London, 20 September.

32. Daniel, Frank Jack, (2012), "India Power Cut Hits Millions, Among World's Worst Outages," Reuters, New Delhi, 31 July.
33. Riley, Charles, (2013), "Hackers Access Federal Reserve Website, Data," CNNMoney, 7 February.
34. www.anz.com/vietnam/en/personal/ways-bank/internet-banking/protect-banking/internet-security-threats/, Retrieved: 2 April 2014.
35. Menn, Joseph, (2013), "Cyber Attacks Against Banks More Severe Than Most Realize," Reuters, 18 May.
36. "Two University Students in Fiji Charged for Laundering \$24,000 from Bank Accounts," Islands Business, 5 February 2014.
37. Agustin, Victor C., (2012), "Hacker Ceans Up Dollar Account in Philippine Bank," 11 August.

References

- Aristotle, (350 B.C.), *Politics*, Greece.
- Basel Committee on Banking Supervision, (2012), “Core Principles for Effective Banking Supervision,” Bank for International Settlements.
- Basel Committee on Banking Supervision, (2011), “Operational Risk – Supervisory Guidelines for the Advanced Measurement Approaches,” Bank for International Settlements.
- Basel Committee on Banking Supervision, (2011), “Principles for the Sound Management of Operational Risk,” Bank for International Settlements.
- Council of Europe, (2001), Budapest Convention on Cybercrime, Strasbourg.
- Deering, S. and R. Hinden, (1998), RFC: 2460, Internet Protocol, Version 6 (IPv6) Specification, December.
- European Union, (2013), “Cybersecurity Plan to Protect Open Internet and Online Freedom and Opportunity,” European Commission, Brussels, 7 February.
- Financial Stability Forum, (2009), FSF Principles for Cross-border Cooperation on Crisis Management.
- Graeber, David, (2011), *Debt: The First 5000 Years*, Melville House, New York City.
- Hasibuan, Zainal A., (2013), “Indonesia Cyber Security Strategy: Security and Sovereignty in Indonesia National Cyberspace,” National ICT Council.
- International Organisation of Securities Commissions (IOSCO), (2013), Principles for Financial Benchmarks.
- Information Sciences Institute, (1981), “RFC: 791, Internet Protocol Internet Program Protocol Specification,” University of Southern California, Marina del Rey, September.
- Juran, Joseph, (2010), *Quality Control Handbook*, 6th Edition, New York.
- Ministry of Communication and Information Technology of India, (2013), National Cyber Security Policy, Proposed 2 July 2013.
- Ministry of Information Communications and Culture of Malaysia, (2014), The National Cyber Security Policy, Available at: nitc.most.gov.my, 1 April.

- National Institute of Standards and Technology (U.S.), (2014), “Framework for Improving Critical Infrastructure Cybersecurity,” Version 1.0, February.
- OECD, (2012), *Cybersecurity Policy Making at a Turning Point - Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy*.
- Office of the Superintendent of Financial Institutions Canada, (2013), *Annex - Cyber Security Self-Assessment Guidance*.
- Rapp, Ronald, J.; Franz-Stefan Gady; Sarabjeet Singh Parmar and Karl Frederick Rauscher, (2012), “India’s Critical Role in the Resilience of the Global Undersea Communications Cable Infrastructure,” *IDSA*, Volume 36, Issue 3, Commentaries: New Delhi.
- Rauscher, Karl Frederick and Yonglin ZHOU, (2011), “China-U.S. Bilateral on Cybersecurity: Fighting Spam to Build Trust,” *EWI and the Internet Society of China (ISC): New York City - Beijing*.
- Rauscher, Karl Frederick and Yonglin ZHOU, (2013), “China-U.S. Track 2 Bilateral on Cybersecurity: Frank Communication and Sensible Cooperation to Stem Harmful Hacking,” *EWI and the Internet Society of China (ISC): New York City – Beijing*.
- Rauscher, Karl. F., (2004), “Protecting Communications Infrastructure,” *Bell Labs Technical Journal Homeland Security Special Issue*, Volume 9, Number 2.
- Rauscher, Karl Frederick, (2010), “The Reliability of Global Undersea Communications Cable Infrastructure (ROGUCCI) Report,” *IEEE*, New York City.
- Rauscher, Karl Frederick, (2010), “The Rise of the 8th Ingredient- the Imperative of Addressing the International Policy Gap in Cyberspace,” *FIRST Technical Colloquium*, Beijing.
- Rauscher, Karl Frederick and Erin Nealy Cox, (2013), *Measuring the Cybersecurity Problem*, East-West Institute.
- Spiotta, A. H., (2003), “Financial Account Aggregation: The Liability Perspective,” *Fordham Journal of Corporate and Financial Law*, Vol. 8(2), p. 557.
- The White House, (2013), *U.S. President Executive Order - Improving Critical Infrastructure Cybersecurity*, Washington, D.C., 12 February.

Consolidated Supervision: Achieving a 360 Degree View of Bank Risk

By Mohd Zabidi Md Nor* and Michael J. Zamorski**,¹

1. Background and Introduction

In recent decades, the landscape of the banking industry has significantly transformed as banks seek to expand their geographic reach, realise economies of scale and scope, diversify their risks and revenue sources, respond to competition, and meet the needs of their clientele. In a 2003 IMF working paper, these trends have been described as the consolidation, internationalisation and conglomeration of banks,² whereby banks are increasingly becoming part of large, multi-tiered groups with complex organisational/ownership structures with international operations.

These groups include:

- a. Banking groups, which provide traditional banking services focused on deposit-taking and lending; and
- b. Financial conglomerates, which conduct banking business while also engaging in other financial activities such as insurance and investment banking.

For purposes of this paper, these two groups will be collectively termed as ‘financial groups’. In addition to financial groups, mixed activity groups – where a bank or a financial group is part of a wider group undertaking commercial activities – also exist, although they may be limited by regulation or less common in some jurisdictions. While many of the issues discussed in this paper are applicable across both types of groups, some are more relevant in the context of mixed activity groups, which are further discussed below in the context of conflicts of interest and the permissibility of non-financial activities in groups.

The spectrum of activities undertaken by financial groups can thus be very broad; some may be under the oversight of certain authorities, while others may be unregulated. Furthermore, given the frequently multinational nature of large groups, their size and inter-linkages may make them systemically important at the global level, and also domestically in individual jurisdictions.

Gaps or weaknesses in the supervisory oversight of both banking and non-bank affiliates, lack of information on cross-border banks and non-bank affiliates, unregulated activities, or other opacities within a financial group may inhibit the timely detection of financial weaknesses or excessive risks, or present opportunities for regulatory arbitrage. Also, there is scope for contagion risk, whereby problems in non-bank affiliates may spread and adversely impact the prudential soundness of other constituent entities, including the bank within the financial group.

Consolidated supervision of financial groups to which banks belong is a long-standing principle of effective banking supervision. In order to effectively identify,

measure, assess and control risks in these typically complex organisations, bank supervisors require:

- a. Access to timely, reliable information on the risks, potential threats and vulnerabilities to banks' safety and soundness posed by affiliate relationships;
- b. The ability to examine the activities of affiliates to understand their nature of business and the risks they pose;
- c. Legal authority to collaborate and exchange confidential supervisory information with relevant domestic and foreign authorities; and
- d. Legal authority to prevent or correct unsafe or unsound practices or conditions arising from affiliate transactions and relationships.

Asia-Pacific countries are both home and host jurisdictions for large, geographically dispersed banks that are part of financial groups operating extensive networks in the region. The effective implementation of consolidated supervision by national authorities is therefore important in promoting regional financial stability.

The IMF has previously expressed concerns about weaknesses in countries' practices related to consolidated supervision identified during their Financial Sector Assessment Program (FSAP) country reviews.³ Improvement opportunities in this area continue to be cited in FSAP reports.

2. Objectives

This article provides a brief historical review of the evolution of international standards relating to consolidated supervision and highlights key policy considerations and challenges in implementing consolidated supervision.

3. Evolution of International Standards for Consolidated Supervision

Before the advent of the international standards covering the key elements of a consolidated supervision framework, national authorities typically relied on national laws and supervisory approaches to address risks arising from a bank's affiliate relationships. The risks were controlled through various mechanisms, including the exercise of examination and inspection authority of bank affiliates, and restrictions on transactions between and among banks and their affiliates.

For example, in the United States, Sections 23A and 23B of the Federal Reserve Act, originally enacted in 1933 and 1987, respectively,⁴ regulate transactions between banks and their affiliates. These laws, which have been revised over the years, include individual and aggregate size limits on affiliate transactions relative to a bank's capital levels, and require that transactions be supported by high quality collateral with conservative margins of protection. Affiliate transactions are also required to be at 'arm's length', that is, on non-preferential terms and conditions, as available in comparable transactions with unaffiliated third parties. Transfers of low quality assets to and between bank affiliates are also prohibited.

Affiliate transaction limitations in the U.S. have been supplemented by providing bank regulators with broad discretionary powers to conduct examinations of any affiliate, or entity deemed to be an affiliate, in order to fully understand the nature of the affiliate relationships, and risks posed by transactions between banks and their affiliates.

Over the last forty years, however, various international supervisory standard-setters, primarily the Basel Committee on Banking Supervision (BCBS) and the Joint Forum have collaborated on developing standards and sound practices related to consolidated supervision. A background summary of their major work follows.

Basel Committee on Banking Supervision – Early Work Related to Consolidated Supervision

The Basel Committee, founded in late 1974, is the international standard setting body for prudential regulation and supervision of the banking industry. The Basel Committee is hosted by the Bank for International Settlements (BIS), Basel, Switzerland, which is owned by the world's central banks and monetary authorities.

One impetus for the founding of the Basel Committee, which was originally known as the Committee on Banking Regulations and Supervisory Practices, was the mid-1974 failure of Bankhaus Herstatt, Cologne, Germany, which had significant cross-border spillovers. Counterparty banks in multiple jurisdictions sustained substantial losses on open foreign exchange contracts that were not settled at the time of its demise.

The lessons from the Herstatt debacle are evident in the Basel Committee's September 1975 "Report on the supervision of foreign establishments – Concordat", known as the Basel Concordat.⁵ One of the Basel Committee's earliest pronouncements, the main objective of the Concordat was "...to set out certain guidelines for cooperation between national authorities in the supervision of banks' foreign establishments" to ensure that no foreign banking establishment escapes supervision. The Concordat also outlined early principles for home and host country information-sharing and cooperation in the supervision of cross-border banks.

The Basel Committee issued a March 1979 paper⁶ entitled "Consolidated supervision of banks' international activities", which expanded on the 1975 Concordat, emphasising the importance of both consolidated and legal entity views of risk, stating:

"...it should be a basic principle of banking supervision that the authorities responsible for carrying it out cannot be fully satisfied about the soundness of individual banks unless they are in a position to examine the totality of each bank's business worldwide. At the same time the Basel Committee recognises that supervisors will also need to continue to look at banks' accounts on a non-consolidated basis."

a. The Joint Forum on Financial Conglomerates

The Joint Forum on Financial Conglomerates (renamed the Joint Forum in 1999) was established in 1996 by the Basel Committee, the International Association of Insurance Supervisors (BIS-hosted standard setter for insurance supervision), and the International Organisation of Securities Commissions. The Joint Forum's mandate is to identify impediments to, and ways of achieving, effective cross-sectoral, cross-border information-sharing, enhanced supervisory coordination among the various regulators of financial groups, and the development of "principles toward the more effective supervision of regulated firms within financial groups."

The Joint Forum's work spanned several years and involved extensive public and industry consultation. A paper entitled "Supervision of Financial Conglomerates," representing a compendium of the Joint Forum's substantial work, was jointly endorsed and issued by the sponsoring committees in February 1999. That paper, supplemented by additional papers published in December 1999, together formed what is known as the Joint Forum's "1999 Principles."

b. Basel Committee's Expanding Coverage of Consolidated Supervision

The Basel Committee is perhaps best known for its substantial and ongoing work on the development and promulgation of international capital standards. However, the Basel Committee has done important work in identifying the essential preconditions necessary for regulatory jurisdictions to have effective bank supervision programs in producing the "Core Principles for Effective Supervision" (known as the Basel Core Principles or BCP), originally issued in 1997, and revised in 2006 and 2012.⁷

The 1997 BCP identified "twenty-five basic Principles that need to be in place for a supervisory system to be effective." Core Principle (CP) 20 states that "An essential element of banking supervision is the ability of the supervisors to supervise the banking group on a consolidated basis." Other CPs in that pronouncement also covered key considerations related to conducting consolidated supervision.⁸

Countries were encouraged to perform BCP self-assessments to identify and remedy any gaps in their supervisory processes. The IMF and the World Bank commenced their Financial Stability Assessment Program (FSAP) reviews in 1999, which included detailed reviews of countries' compliance with the BCP.

The BCP were updated in October 2006, retaining the same number of CPs, to acknowledge changes in banking regulations, new regulatory insights, identified gaps in regulation and experience in applying the BCP during FSAP reviews. CP 20 from the 1997 BCP, covering Consolidated Supervision, was expanded into two CPs:

CP 24	Consolidated supervision: An essential element of banking supervision is that supervisors supervise the banking group on a consolidated basis, adequately monitoring and, as appropriate, applying prudential norms to all aspects of the business conducted by the group worldwide
CP 25	Home-host relationships: Cross-border consolidated supervision requires cooperation and information exchange between home supervisors and the various other supervisors involved, primarily host banking supervisors. Banking supervisors must require the local operations of foreign banks to be conducted to the same standards as those required for domestic institutions

The BCPs were revised again in September 2012, incorporating lessons learned from the global financial crisis of 2007-08. The number of CPs was expanded from 25 to 29. The text of CP 24, Consolidated Supervision, has been retained verbatim, except it has been reordered and is now CP 12.

Each of the CPs specifies Essential Criteria (EC) and Additional Criteria (AC) to be considered in assessing compliance. “Essential criteria set out minimum baseline requirements for sound supervisory practices and are of universal applicability to all countries”.⁹ While the EC are mandatory, “...countries undergoing FSAP assessments by the IMF and/or World Bank can elect to be graded against the essential and additional criteria”¹⁰ The references for the detailed EC and AC pertaining to CPs 12 and 13 are provided in the endnotes.¹¹

At the same time, other CPs also acknowledge the importance of banking groups and supervisors in assessing the effectiveness of the risk management framework on a group-wide basis to cover exposures undertaken by the bank and its affiliates, including entities which operate as part of the wider group. This includes ensuring that processes which facilitate group-wide monitoring and control of risks (e.g. credit, market, liquidity and operational risks) are in place and are consistent with the risk profile, risk appetite and systemic importance of the bank and the group to which it belongs.

4. Regulatory Performance in Implementing Consolidated Supervision

The development of the BCPs has enabled a global overview of progress towards developing an effective consolidated supervision framework across jurisdictions. In this respect, a September 2008 IMF paper reviewed the results of 136 FSAP assessments of countries’ compliance with the original (1997) version of the BCPs. The 1997 BCPs require, under CP 20, Consolidated Supervision, that “...supervisors have the ability to supervise the banking group on a consolidated basis, whereby all risks run by a banking group are taken into account, wherever they are booked.” Regarding CP 20, the IMF review stated that:

“Although 44 percent of the assessed countries are rated noncompliant,¹² the figure could be greater as another 20 percent were not assessed on this principle or this was deemed to be ‘not applicable’ to their financial systems on the grounds that formal structures were not present. Commonly-cited deficiencies were the lack of reliable consolidated information or legal powers to examine and supervise some activities, including those of offshore banks; inability to have direct access to nonconsolidated subsidiaries and to the holding company; no capital allocation to cover risks on a consolidated basis; no framework to evaluate risks presented by non-bank entities within a group; no provisions or arrangement to share information with other supervisors (domestic or foreign) of group entities; no legal requirements to consolidate the operations of all subsidiaries and report the accounts and exposure on a consolidated basis; and no requirement to report prudential requirements on a consolidated basis.”¹³

Twenty-three BCP assessments were published by the IMF/World Bank during 2012 and 2013 which were based on the 2006 BCP assessment criteria. Assessed countries were diverse with respect to their size and stage of development; many of the countries had undergone one or more previous FSAP assessments. Surprisingly, the assessments disclosed noncompliance with some basic standards contained in CPs 12 and 13, for example:

- a. The lack of legal authority to review the overall activities of a banking group;
- b. No legal authority to exchange confidential supervisory information with foreign supervisors;
- c. Possessing, but not exercising, legal authority to review group information; and
- d. The absence of information-sharing arrangements, such as Memorandums of Understanding (MOUs), despite significant overseas operations and significant foreign bank presence in the home country.

There have been six IMF/World Bank BCP assessments published to date, beginning in late 2013, which were based on the 2012 BCP revised assessment criteria.¹⁴ These recent assessments reflect that the reviewed jurisdictions are mostly “compliant” and at least “largely compliant” with CPs 12 and 13.¹⁵

5. Key Policy Considerations

While the overarching principles of an effective consolidated supervision framework have been continually enhanced by international standard setters, national regulatory and supervisory authorities remain confronted with the challenge of translating these broad concepts into policies which are appropriate within their respective jurisdictions.

In recent years, overcoming this challenge has become increasingly important due to the expansion in both scale and scope of the activities carried out by banks

across the globe. As national authorities seek to accelerate efforts to strengthen their oversight of banks, particularly in emerging markets where such trends are likely to further materialise at a rapid pace, having a clear understanding of key policy considerations will be crucial to the successful implementation of consolidated supervision.

Risks that Consolidated Supervision Seeks to Control

Consolidated supervision seeks to ensure that supervisors are able to develop a more comprehensive group-wide assessment of risks arising from the activities of a bank's affiliates while ensuring that these risks are prudently managed. The following discussion illustrates how affiliate relationships and transactions can lead to serious problems if they are not properly monitored and controlled.

a. Excessive Leverage and Double-leveraging of Capital

At a very fundamental level, leverage is the extent to which an entity borrows to fund its assets. Leverage gives rise to debt servicing obligations, which can place substantial strain on the finances of an entity in stressed conditions. The risks associated with excessive leverage can therefore be intensified within the context of banks, as their role as credit intermediaries requires them to borrow – at a magnitude unlike other real sector businesses – from surplus savers to enable the provision of credit in the real economy.¹⁶

One of the supervisory tools in managing this risk is the application of capital adequacy requirements or prudential limits on the banking entity. On its own, however, an entity-focused approach to assessing the balance sheet leverage of the bank is often inadequate. Where a bank operates as part of a wider financial group, there may be circumstances whereby such an assessment may not fully capture the effective leverage being undertaken by the bank due to the potentially numerous and complex relationships with its affiliates.

These circumstances have been described at length by the Joint Forum¹⁷ as the following:

i. Where the bank is a subsidiary of an unregulated firm

In this situation, the parent company may issue debt – or other instruments not acceptable as regulatory capital – and down-stream or pass the proceeds to the subsidiary in the form of equity or other elements of regulatory capital.

While this type of leverage is not necessarily unsafe or unsound, it may pose material risks for the bank if undue stress is placed on the bank arising from obligations of the capital issuer to service its debts, or where there is a discrepancy between the quality of capital instruments issued by the parent and those which it downstreams to the bank.

Additionally, excessive leverage can create undue pressures on the bank to sustain high dividend payments to service an excessive debt load of an upstream affiliates, which may, in turn, induce banks to pursue excessively risky or unsafe and unsound business strategies in an attempt to maximise profitability. This risk might be elevated in situations where effective governance might be compromised due to conflicts of interest, which is discussed below.

- ii. *Where one entity holds regulatory capital issued by another entity within the same financial group (i.e. double or multiple leveraging)*

Within the context of the constituent bank, although this amount will count towards its capital and therefore reduce its balance sheet leverage, the same capital is being used simultaneously to buffer against risks in at least two entities within the financial group. Effectively, the leverage of the bank is being potentially understated.

Instances of double or multiple leveraging can therefore be easily obscured in overly complex organisational or ownership structures, which may not be uncommon among large, cross-border financial groups. The key issue, however, is not the organisational or ownership structure per se, but the consequences of the structure for the assessment of the financial group's group-wide capital, which could ultimately reduce the supervisability of the financial group.

- iii. *Where there are unregulated affiliates within the financial group*

There is also a need to consider risks undertaken by other unregulated non-bank affiliates, such as its sister companies, special purpose vehicles and other off-balance sheet entities. Notwithstanding the establishment of firewalls within the financial group, the activities undertaken by non-bank affiliates may be a channel for contagion (discussed further below). Again, the balance sheet approach to assessing leverage fails to fully consider such a situation.

For these reasons, the BCBS requires the Basel capital framework to be applied on a consolidated basis to banking groups, including those headed by holding companies and also at every tier within a banking group. At the same time, banking entities are also expected to be adequately capitalised on a standalone basis.¹⁸

b. Contagion Risk

Contagion risk refers to the transmission of risks across entities in the group through different forms of economic linkages. From the perspective of a banking supervisor, this is a key concern as losses or adverse events affecting an affiliate may result in difficulties for an otherwise prudent and sound bank.

A key channel for contagion risk are financial relationships arising from intra-group transactions, exposures and legal arrangements between the bank and its

affiliates. Centralised liquidity management can be such an example. The pooling of liquidity and funding arrangements suggest that such risk-sharing arrangements allow financial groups to manage liquidity risk more efficiently, as compared to a situation where liquidity pools are ‘trapped’ in subsidiaries. Nonetheless, these benefits have to be weighed against other concerns, including that of moral hazard, which are discussed in the following sections. For instance, the recent Eurozone crisis demonstrated that parent companies of cross-border financial groups may have a tendency to transfer funds from financially healthy subsidiaries to affiliates facing liquidity problems.¹⁹

Reputational associations may also be a potentially material channel of contagion, as legal and operational demarcations may not be immediately apparent to market participants, such as the general public and credit ratings agencies. Depositors, for example, may – whether rightly or wrongly – associate the financial position of a bank with that of its affiliates due to shared branding. To a large extent, assessments by credit rating agencies of entities within a financial group, such as the holding company, are also influenced by the risk profile of the constituent bank. Likewise, problems or concerns with such affiliates may also weigh down the credit ratings of a bank which is otherwise sound on a standalone basis.

From the perspective of the bank and its parent company, reputational associations may incentivise management to exert efforts to protect the franchise value of the shared branding. In this case, there may be a need to safeguard and protect the financial group’s reputation, and to preserve longstanding customer relationships. This further intensifies the need for intra-group support even if this comes at the expense of the constituent bank.

Other financial arrangements which interlock the safety and soundness of a bank with the operations of its affiliates include guarantees provided by the constituent bank to its affiliates as well as cross-default clauses that are incorporated into the terms of issuance of debt obligations and derivative contracts by any entities within the group. Loan participations originated and sold to affiliated banks can also be a source of contagion in the event of deterioration in a borrower’s ability to repay or other adverse developments impacting collectability.

c. Conflicts of Interest May Undermine Corporate Governance or Induce Excessive Risk-taking

The sheer breadth in the scope of activities undertaken by a financial group expands the avenues for conflicts of interest, as the financial group will have to consider interests of not just the constituent bank, but also those of other subsidiaries or affiliates. Central to this issue are situations whereby the bank’s interests – and hence, possibly the public’s interests – may be compromised in order to advance the financial group’s overarching business strategy or profitability.

Potential conflicts of interest are likely to surface when there is a significant amount of intra-group transactions and exposures, such as through:

- i. Lending on terms and conditions or prices which are not at arm's length with the intention of providing financial support to an affiliate;
- ii. The payment of royalties and fees for services provided by an affiliate; and
- iii. Self-dealing, whereby a constituent entity in the financial group acting as a fiduciary is a party to a transaction with itself or its affiliates (e.g. different entities within the same financial group providing brokerage advice to a client as well as executing the trading of securities on which advice is being given).

The magnitude of conflicts of interest within a financial group may escalate as more complex intra-group relationships are established to fully realise the synergies arising from different businesses within the group. Such interlocking relationships may obscure the lines of accountability and the mechanisms by which control is exercised over entities within the group, including the constituent bank. For example, reporting lines and information flows between the bank, its parent company and/or other subsidiaries may not be sufficiently clear for supervisors to develop an adequate view on whether internal controls and processes are robust enough to mitigate conflicts of interest and to form an overall conclusion of the risk profile of the financial group.

Conflicts of interest may also arise within the context of a cross-border banking financial group which has separately capitalised banking subsidiaries in multiple countries. This may happen when the corporate governance practices within the group are weak or where the regulatory requirements, such as those relating to connected party lending and large exposure limits, are not adequately applied at the consolidated level. Under such circumstances, the parent bank within the financial group could potentially circumvent lending limits imposed by the home supervisory authorities by mandating the participation of its affiliated banks in other jurisdictions in a particular financing scheme.

This is particularly relevant in circumstances where certain scope of decisions are made by a centralised credit approval committee either at a regional or global level, instead of the individual affiliated bank operating in the host jurisdiction. Some internationally-active financial groups, for example, subject loan applications above certain thresholds to such an approval process. These actions may be incongruent with the banking subsidiary's own risk appetite or may undermine the fiduciary duties and responsibilities of the board of directors to act in the best interests of each banking subsidiary's depositors, minority shareholders and other creditors.

Where a bank belongs to a mixed activity group with material non-financial undertakings, such as an industrial conglomerate, the risk for conflicts of interest may also be heightened. In particular, the role of the constituent bank in the group's overall business strategy may be to primarily support the interests of the other entities carrying

out commercial activities, particularly where such activities – rather than those of the bank – are the underlying drivers of the group’s profitability and growth.

While such a setup is intended to realise the resultant synergies of having a bank in the group – there can be instances where serving the commercial or strategic interests of the group comes at the expense of the bank’s and that of its depositors. For example, the constituent bank may be unduly pressured by the parent company to provide financing to commercial affiliates at preferential rates. Strong informal relationships with the management of other affiliates may also result in a lack of impartiality in the bank’s credit decisions due to strong informal relationships. Applying effective consolidated supervision for such a group structure would be more challenging. For this reason, many jurisdictions have taken measures to restrict such structures, as set out in the subsequent section, “Defining the Perimeter of Consolidated Supervision.”

d. Oversight of Excessive Risk-taking by Affiliates Arising from Moral Hazard

Non-bank affiliates may wrongly perceive that, given the substantial economic inter-linkages between their operations and the bank, the central bank’s lender-of-last-resort facilities are likely to be extended to them in times of stress, whether directly or indirectly. This could create incentives for non-bank or unregulated affiliates within the group to undertake excessive risks, which is a situation described as moral hazard. This is more likely where the financial group or the bank in question is considered as being systemically important or ‘too-big-to-fail.’

Identifying this risk is however not easy in practice. Entity-level regulation and supervisory oversight may not be adequate to help bank supervisors detect excessive accumulation of risks at non-regulated affiliates at a sufficiently early stage to facilitate supervisory intervention. This is therefore the argument in advancing a consolidated supervision framework to allow bank supervisors to have a group-wide view of the financial group and adopt a more proactive approach to supervision. At some level, the application of prudential regulation on a consolidated basis may also provide incentives within the financial group to better align the group business strategies to be consistent with the risk-taking capacity of the individual constituent entities, including non-bank or non-regulated entities.

Defining the Perimeter of Consolidated Supervision

Given the wide array of risks to banks arising from the operations undertaken by its affiliates, it is imperative that supervisors clearly define the appropriate regulatory and supervisory perimeter of financial groups. Conceptually, this perimeter should capture any affiliates which may potentially give rise to the aforementioned risks. In practice, this is likely to entail tracing the lines of ownership to the top of the shareholding structure, namely the controlling entity or ultimate parent company of the group in which a bank resides. In this case, the parent company and all its downstream entities

will be defined to be within the perimeter of consolidated supervision. Additional considerations, however, may emerge due to the potentially significant variations in the way groups are structured.

a. Permissibility of Non-financial Activities

One such consideration arises in the context of mixed activity groups, namely where a bank is part of a wider group with undertakings in non-financial activities, such as an industrial conglomerate engaging in real sector activities or a sovereign wealth fund with significant investments in non-financial firms. In this instance, tracing the lines of ownership to the top of the shareholding structure could result in expanding the scope of oversight to cover activities which may not be traditionally under the ambit of any prudential authority, be it in banking, insurance or securities.

Where these non-financial activities are material and share significant economic relationships with the bank, there may be a need to assess the extent to which such activities are permissible in the banking group. In particular, supervisors will have to weigh the potential benefits of allowing banks to be affiliated with a wider scope of activities – such as operational synergies that offer greater growth potential for business and customers, as well as diversification benefits from allowing banks to be affiliated with a wider scope of activities – vis-à-vis key supervisory and market competition concerns.

These concerns which reflect risks mentioned in previous section may include, but are not limited to:

- i. Greater scope for contagion risk, which may arise from increased pressure by shareholders to support non-financial affiliates;
- ii. Potential exposure to political influence, particularly where financial groups carrying out non-financial activities are large and affiliated with the government or other special interest groups;
- iii. Potential impact on market competition in the non-financial activities undertaken within the group given the position or significant roles of the affiliated banks in the economy;
- iv. Potential inherent limitations in supervisory capacity to develop comprehensive assessments of commercial risks, compounded by a more dynamic and complex environment;
- v. The challenge to determining adequate prudential safeguards to limit spillover of risks arising from non-financial activities to the bank without materially eroding the synergies of operating within such an ownership structure in the first place; and
- vi. Complexity of resolution and recovery planning for the affiliate banks when non-financial activities are involved.

The complexity in balancing these trade-offs is illustrated by the lack of clear consensus or common regulatory policies on whether involvement in non-

financial activities should be explicitly allowed, restricted or prohibited. The exercise of supervisory discretion in determining appropriate policy responses in this area reflects the delicate situation and unique circumstances faced by supervisors in individual jurisdictions. In many jurisdictions where prudential restrictions or limits are applied, these are primarily intended to avoid risk concentration and do not distinguish between the different types of non-financial activities in which banks may be engaged (Table 1). To some extent, such restrictions may therefore be used by supervisors to limit the exposures of banks to risks from other commercial risks undertaken by the group.

Table 1²⁰

Jurisdiction	Investments Made by Banks	Ownership in Banks
Australia	Subject to limits	Subject to approval
Canada	Subject to limits	Subject to limits
China	Subject to limits and approval	Subject to approval at the 5 percent threshold
European Union	Subject to limits	No general restrictions, but subject to approval at the 10 percent threshold
Hong Kong	Subject to limits	Subject to approval at the 10 percent threshold
Japan	Subject to limits	Subject to approval at the 20 percent threshold
Malaysia	Subject to limits	Subject to approval at the 5 percent threshold
Phillippines	Subject to limits	Permitted but subject to limits
Singapore	Subject to limits on individual investments and subject to approval at the 10 percent threshold	Subject to approval at 5 percent, 12 percent and 20 percent threshold
United Kingdom	Subject to supervisory consultations	No statutory prohibition
United States	Subject to limits and regulatory restrictions	Permitted to make non-controlling investments

In addition, some countries have also developed more robust legal frameworks and regulatory policies to impose some restrictions on individuals, groups of individuals or corporations that own or control a bank. These measures may be aimed at addressing potential risks arising from the ownership of a bank by a shareholder significantly involved in non-financial activities. For example, some jurisdictions have extended the supervisory reach by adopting a wider legal definitions of ownership 'control' to which prudential limits may be applied to include situations where such controllers do not even have 100 percent equity ownership or even a majority of voting shares. In the United States, for example, the threshold for controlling ownership is 25 percent under the Bank Holding Company Act of 1956.

Similarly, individuals whose personal shareholdings do not meet defined control thresholds may nevertheless be deemed to exercise a “controlling interest” or be part of a group based on a regulatory determination that the group members, acting in concert, exercise a controlling influence.

To the extent that non-financial activities are allowed to be undertaken by the wider corporate group (i.e. outside the financial group subject to consolidated supervision), there remains the need for supervisors to assess risks arising from such activities.²¹ As prudential supervision is not typically applied on non-financial activities, substantial capacity building efforts may be required to broaden the supervisory scope of knowledge to cover commercial activities carried out by the bank’s affiliates. This entails developing a comprehensive understanding of the nature of these activities to identify risk channels through which the safety and soundness of the constituent bank may be affected. Furthermore, supervisors will have to put in place adequate arrangements which enable access to critical information on these commercial activities to facilitate early identification of risks and intervention actions where appropriate.

b. Foreign-owned Groups

Within the context of internationally active groups, concerns may also exist from the perspective of host supervisory authorities, in view of the Basel Concordat which accords the home supervisory authority the role of consolidated supervisor. Notwithstanding the international regulatory framework, supervisors in their capacity as host authorities may view that there is a need to conduct consolidated supervision over operations by the bank and its affiliates which are undertaken in the host jurisdiction, particularly if these operations are collectively assessed to be systemically important to the stability of the local financial system or if equivalent prudential oversight by home authorities is not deemed to be equivalent (see Table 2).

Beginning 2015, the United States, for example, will require the formation of an intermediate holding company, effectively subjecting the group’s operations in the United States to the Federal Reserve’s consolidated supervision, if the global assets of the group exceed \$50 billion and if non-branch assets in the United States exceed \$50 billion.

Table 2

Authority	Treatment of Foreign-owned Groups
Australia	Does not require formation of locally-incorporated holding companies
European Union	<ul style="list-style-type: none"> • Requires the verification of equivalent home supervision • In the absence of equivalent home supervision, consolidated supervision will apply on the foreign group • Will designate a locally-incorporated holding company if any

Authority	Treatment of Foreign-owned Groups
Malaysia	<ul style="list-style-type: none"> • In general, does not require formation of locally-incorporated holding companies • Subject to an assessment of existing prudential arrangements and the systemic importance of the foreign-owned group's local operations
Singapore	<ul style="list-style-type: none"> • In general, does not require formation of locally-incorporated holding companies • Subject to an assessment of the significance of local operations to the local financial system or the global financial group, and the extent of group-wide supervision by home supervisory authorities
United States	<ul style="list-style-type: none"> • Subject to US enhanced prudential standards if global assets of foreign banking group exceed US\$50 billion • Requires formation of intermediate holding company if non-branch US assets exceed US\$50 billion

c. Scope of Regulatory Consolidation

There is also the need to determine the appropriate scope of consolidation. In this regard, international accounting standards provide a useful baseline in defining the appropriate scope of consolidation (and hence, the entities which should be captured within the perimeter). In particular, the concept of control underlying accounting consolidation, which requires the establishment of the investor's power over and rights to variable returns from the investee, are likely to allow supervisors to cast a sufficiently broad net to capture the relevant entities for consolidated supervision.

Nonetheless, there might be circumstances where accounting consolidation may not sufficiently reflect the range of relationships or magnitude of certain types of risks within the financial group which may be relevant for purposes of supervisory assessments. Robust supervisory oversight therefore requires an in-depth understanding of the economic relationships embedded between a bank and its affiliates, including those in the wider group,²² and how these relationships may translate to become potential risk channels. For instance, accounting consolidation may not capture the reputational risks arising from brand associations that could potentially undermine an otherwise prudent and sound bank. While such situations may be very remote, supervisors may need to expand the scope of consolidated supervision in order to obtain additional information, impose specific restrictions or conduct examinations of any affiliates that may pose potential risks to the bank.

d. Amplification of Moral Hazard

The potential for moral hazard arising from the association of non-bank or non-regulated entities with banks may be further amplified by the policy to draw clear boundaries for consolidated supervision. The explicit definition of the scope of oversight under consolidated supervision – whether by legal powers, regulatory requirements or supervisory activities – may have implications on public perception,

which, if not properly managed, can be counterproductive to the one of the intended objectives of consolidated supervision, namely to address moral hazard itself.

In practice, the moral hazard problem could be amplified by way of public and investor expectations relating to the relationship between the bank supervisor and non-bank affiliates. Where once there was merely a perceived extension of the public sector safety net to non-bank affiliates, the establishment of a consolidated supervision framework with a clearly-defined scope of group-wide oversight may be understood by the public as a confirmation of this relationship. This, in turn, can create further misconceptions that, moving forward, non-bank affiliates will be under the same rigour and magnitude of oversight as that applied to banks, thus creating an unfair advantage for the non-bank affiliates. For example, when non-bank affiliates undertake capital-raising activities, the funding provided to them may be underpriced as investors and credit ratings agencies assume an equivalent risk profile between the bank and its non-bank affiliates. This could be further compounded in the context of internationally-active groups, as home authorities may be expected to expand the coverage of the public sector safety net, such as deposit insurance or emergency liquidity assistance, to banking operations being undertaken in host jurisdictions. It should be noted, however, that historically, there is no strong precedent of a cross-border extension of any of these safety nets.

It is therefore important that regulatory and supervisory authorities take appropriate steps to ensure sufficient policy clarity in communicating the intent and focus of consolidated supervision to the financial groups, market participants as well as the public at large. In this respect, it should be clear that the oversight of a bank's affiliates is only relevant to the extent that it serves to safeguard the interests of the public, namely depositors and insurance policyholders.

Adequate Legal Powers, Inter-agency Arrangements and Supervisory Capacity to Conduct Consolidated Supervision

While defining the regulatory and supervisory perimeter provides clarity on the scope of consolidated supervision, adequate legal authority is most critical in enabling supervisors to conduct such group supervision effectively. Of particular importance is the need for clear and explicit powers to identify sources of material risks to the bank or financial system stability and to undertake corrective actions in a timely manner.

Since regulatory and supervisory powers have traditionally been focused on the regulated bank and its subsidiaries, consolidated supervision will require oversight powers of the legal framework to be extended, in particular to the parent or holding company of the banks to enable supervisors to develop a more complete understanding of the relationships and risks within the entire group.

Such broad powers typically entail provisions to regulate and supervise the holding company which exercises control over banks and their affiliates, particularly in cases where the ultimate parent company of the bank is a non-regulated entity. The

specific approach in achieving these oversight powers, however, does not necessarily have to be identical across jurisdictions for consolidated supervision to work. Supervisors in Singapore, for example, may designate financial holding companies through which consolidated supervision is conducted. Meanwhile, in Malaysia, holding companies of licensed institutions, including banks, need to be approved under the law, which effectively subjects them to regulatory and supervisory oversight.

Notwithstanding the differences in the legal framework, the intended outcome is achieved where the holding company serves as a supervisory point of entry to access information on other entities within the financial group – which in turn guides supervisors in forming a group-wide risk assessment – as well as to implement group-wide prudential rules on a consolidated basis. In ensuring that the potential opacity or complexity of group structures does not impede a clear view by supervisors of the global and consolidated operations of a group – hence the consolidated supervision perimeter – powers to require restructuring may also support the implementation of regulatory requirements and supervisory activities.

It is also particularly vital to ensure that supervisors and other relevant authorities have sufficient capacity to provide for the resolution of banks within the context of financial groups.²³ The level of such capacity may be greater than traditionally required to resolve banks on a standalone basis. This may arise due to the added complexity arising from, among others:

- i. The operational dependencies of the constituent bank with affiliates carrying out centralised functions for the group;
- ii. The cross-border nature of a financial group's operations, legal constraints on the exchange of information among constituent entities of a financial group; and
- iii. The potentially higher degree of interconnectedness with the financial system.

These challenges have prompted further debate among policymakers on how the building blocks of national resolution regimes should be strengthened within the context of financial groups. Some have suggested the adoption of 'single point of entry' solutions, where resolution powers – such as bail-in or transfer tools – are applied at the holding company level by a single resolution authority and losses incurred in the group are absorbed by the holding company.²⁴ Nonetheless, others maintain that a 'multiple point of entry' approach, where subsidiaries are individually resolved by various resolution authorities, remains appropriate.

Given the wide span of activities undertaken by a financial group, it is crucial that there is a clear delineation of formal roles and responsibilities of the different authorities, both domestically and internationally.

In the domestic context, the pertinence of developing arrangements to facilitate consolidated supervision largely depends on whether both banking and insurance sectors are under the oversight of a single prudential authority. This is the case in jurisdictions such as Australia, Singapore, Indonesia and Malaysia. However, where

banking institutions and insurers are under the ambit of different oversight authorities – such as in Thailand, Hong Kong, China and the Philippines – there will be a need to clearly establish which authority is primarily responsible for conducting consolidated supervision while setting out the roles and functions of other authorities in the overall framework for group oversight, particularly with regard to information sharing arrangements as highlighted by the Joint Forum.²⁵ The division of responsibilities may be legislated (as is the case in Europe and the United States), although a similar outcome can also be achieved through a Memorandum of Understanding between the relevant authorities.

In this regard, the institutional arrangements in the United States are instructive. For example, the Federal Reserve has important oversight responsibilities over deposit-taking institutions, while also acting as the ‘umbrella supervisor’ for purposes of consolidated supervision. In its capacity as the lead regulator, the Federal Reserve focuses on the holding company on a consolidated basis, while placing reliance on ‘functional regulators’ (e.g. the Securities Exchange Commission, Commodities Futures Trading Commission, etc.) to provide information on non-depository affiliates under their oversight. The Federal Reserve also closely coordinates with the Office of the Comptroller of the Currency and Federal Deposit Insurance Corporation, the primary regulators for the banks under their jurisdiction, to share information on banks that have holding company affiliations or are systemically important.

Nonetheless, formal arrangements alone are insufficient, as demonstrated by the experience of the United Kingdom during the crisis, whereby the Memorandum of Understanding between the Bank of England, Financial Services Authority and HM Treasury – better known as the tripartite arrangement – was not able to facilitate adequate intervention to effectively fulfill its financial stability objectives. This experience highlights the crucial need for adequate powers and tools to directly enforce timely corrective actions on any constituent entities of the financial group, if they have been assessed to be unduly exposing the bank or financial system stability to material risks.²⁶

For financial groups with significant cross-border operations, effective home-host arrangements are crucial.²⁷ While practices in this area have evolved over the recent years to facilitate the sharing of experience among supervisors globally, practical impediments may surface for many supervisors in emerging economies, preventing them from fully leveraging on these arrangements. This can occur where a financial group’s activities in a host jurisdiction are insignificant to the home authority but systemically important to the host authority. This is not uncommon in emerging markets, in which many large internationally-active financial groups operate. In this instance, the host authority may be excluded from, or unable to participate meaningfully in, appropriate platforms such as supervisory college meetings or crisis management groups to escalate its local supervisory concerns, especially those relating to risks from non-bank affiliates.

Hence, formal home-host arrangements need to be complemented with a strong underlying relationship. The development of such a relationship demands that a culture

of mutual trust and reciprocity exists and is being continuously nurtured to encourage the sharing of critical supervisory information which can, at times, be highly sensitive or confidential in nature. This, in turn, requires continuous engagements over time. As financial groups continue to expand at a rapid pace, supervisors too should continue to advance efforts to cement both existing and new home-host relationships through frequent and comprehensive cross-border engagements.

Enhancements to the existing gateways for information-sharing should, however, be pursued to ensure that formal home-host arrangements continue to be relevant in the increasingly dynamic and evolving financial landscape of internationally-active financial groups. This may include putting in place operational capabilities and procedures that facilitate and coordinate the sharing of critical information. Considerations may also be given to the advancement of collective efforts at the international level, such as through the development of multilateral arrangements which provide a framework for international cooperation and coordination. An example of this is in the securities sector where the International Organisation of Securities Commissions (IOSCO) has developed a Multilateral Memorandum of Understanding (MMoU) which sets out general principles related to the scope, nature and operationalisation of cross-border inter-agency cooperation.

In respect of technical capacity, the intensity of consolidated supervision may also require the agency that assumes the role of lead agency to upgrade its supervisory resources. In particular, supervisory teams may need to expand their technical knowledge of risks beyond the traditional realm of banking activities, particularly those carried out by unregulated entities in the financial group. To the extent that these activities are under the oversight of another authority, the lead agency should leverage as much as possible on inter-agency arrangements. The available supervisory infrastructure should also be commensurate with the size of a financial group's operations, which may increase the need for more sophisticated data management capability. This may include the development of, or enhancements to, a centralised system which integrates key supervisory information.

Role and Approach of Entity-level Supervision vis-à-vis Consolidated Supervision

Finally, with a consolidated supervision framework in place, supervisors may need to reassess the appropriateness of the role and approach of entity-level regulation and supervision. From the perspective of global standards, the broad principles related to consolidated supervision so far are articulated within the context of regulating a bank or an insurer – this may suggest a supporting role for consolidated supervision, whereby group-wide requirements are developed as a complement to, not a substitute for, entity-level requirements.²⁸

One may argue that there might be instances where regulatory requirements imposed at the consolidated level could be considered as an adequate substitute for the requirements imposed at the entity level. For example, the case for retaining prudential limits on large exposures to a single counterparty at the entity level could be reviewed

if such limits are already applied on a consolidated basis. Similarly, when applying requirements on capital adequacy or liquidity on a consolidated basis, supervisors' lack of preference over the location and distribution of such resources within the group could suggest the confidence and willingness to rely on rules observed at the consolidated level. Some jurisdictions, such as the European Union, for instance, do provide for the exemption of entity-level liquidity requirements if those requirements are applied on a consolidated basis.²⁹ Likewise, in Brazil, capital requirements are applied on a consolidated basis and do not require a separate test on the capitalisation of individual banks within a financial group.³⁰

While it is incumbent upon supervisors to continually assess the complementarity and compatibility of prudential regulation applied at both entity and consolidated levels, lessons from the recent global crisis however suggest a continuing focus on entity-level supervision while enhancing the quality of consolidated supervision. The 'top down' approach to the assessment of risks within banks, which relies on aggregation of financial data from multiple bank affiliates and even non-bank affiliates while de-emphasising or ignoring legal entity views of risk – as advocated by some supervisors prior to the crisis – may be inadequate. While this approach provides a consolidated set of information on bank subsidiaries' condition and performance, it has shown to be insufficient to help supervisors understand the conditions of affiliated banks from a safety and soundness perspective on a stand-alone basis. A consolidated view of affiliated banks' risks may, for example, reflect adequate capital and liquidity buffers for the group as a whole, but mask the build-up of risks within banking subsidiaries on a stand-alone basis. This analytical approach erroneously assumes that capital and liquidity within a banking group is fungible, such that it can be reallocated among the various subsidiaries at will. This is not always the case due to regulatory or legal restrictions on transactions with affiliates, as well as the need for the boards of directors of affiliated banks to determine, in line with their fiduciary responsibilities, whether the transaction is in the best interests of the bank.

The complexity of banking group operations and the expanding scope of their activities do suggest that the supervisory resources should be directed towards continuously improving the quality of supervision at both the entity and consolidated level. Any policy discourse relating to consolidated supervision should be premised on the fundamental objectives of regulating institutions such as banks and insurers, and how these intended objectives could be better achieved in any manner by changing the current regulatory and supervisory approach.

Conclusions and Recommendations

Over the last decade, the Asia-Pacific region has been experiencing increasing financial integration and many close inter-linkages have developed. This will be further reinforced by regional initiatives, such as the ASEAN Banking Integration Framework, to advance the agenda of creating more competitive, open and internationalised financial sectors. As the region transitions into a more

interconnected phase of development, a key priority for central banks and other oversight authorities moving forward is therefore to ensure that the developments are anchored by regulatory and supervisory regimes which adequately acknowledge the accompanying risks and considerations.

Effective consolidated supervision is one of the central tenets of such a regime, whereby the group-wide operations of large, cross-border financial groups are subject to prudential requirements, including in areas of capital adequacy, corporate governance, risk management and prudential limits. These requirements serve to mitigate regulatory blind spots which can give rise to excessive leverage, contagion, conflicts of interest and moral hazard. Other areas of regulation such as that involving the development of crisis management and group resolution regimes, cross-border safety nets³¹ and structural bank regulation³² must also be considered in enhancing the approaches to consolidated supervision.

In advancing the objectives of effective consolidated supervision, supervisory authorities need to, at a fundamental level, assess and periodically review, given possible changing circumstances, the country's compliance with the "Essential Criteria" of Core Principles 12 and 13 of the 2012 BCP. Action should be taken to remedy any gaps or instances of less than full compliance with the EC. Other critical steps would include ensuring:

- i. Sufficient legal powers exist to allow examination and inspection of banks' affiliated entities;
- ii. Appropriate legal restrictions covering transactions between banks and their affiliates are effectively in place;
- iii. The country's legal and regulatory framework support adequate domestic and cross-border supervisory cooperation and information exchange, including with relevant non-supervisory authorities, such as finance ministries and deposit insurers;
- iv. The operating protocols for the confidential exchange of supervisory information with foreign supervisors are specified in Memoranda of Understanding, and that those agreements emphasise the extreme sensitivity and paramount obligation of all parties to the agreement to protect confidential supervisory information that they receive; and
- v. Home-host relationships are strengthened, particularly in the establishment of effective supervisory colleges by home supervisors for banks that conduct significant cross-border operations.

Each of these areas would require sustained efforts in strengthening both domestic and cross-border relationships and the establishment of structured coordination and information exchange arrangements to facilitate a better understanding of the complexity of each country's economy, legal system, stage of economic development and most importantly, the characteristics and risks of the banking system and wider financial sector.

-
- * **Mohd Zabidi Md Nor** is the Director of Prudential Financial Policy Department of Bank Negara Malaysia. He oversees the development of prudential policies including capital, corporate governance and risk management standards for both banking and insurance sectors as well as for financial groups in Malaysia.

 - ** **Michael J. Zamorski** is an Adviser to Bank Negara Malaysia and SEACEN on Financial Stability and Supervision. He has 33 years' experience in financial institution supervision and regulation and was a bank Chief Risk Officer. As Director of Supervision and Consumer Protection for the U.S. Federal Deposit Insurance Corporation, he was responsible for prudential and conduct of business supervision for 5,200 U.S. banks. Mr. Zamorski was a member of the Basel Committee from 2000-2006 and of the Basel Consultative Group during 2009-2010.

Endnotes

1. We wish to express our appreciation to Lee Zhi Wei for his invaluable support in respect of research and drafting of this article. We also thank Bank Negara Malaysia's Assistant Governor, Jessica Chew Cheng Lian for her constructive comments and kind suggestions. The observations, analysis and recommendations contained in the article are the perspectives of the authors and do not reflect in any way the views of Bank Negara Malaysia or The SEACEN Centre.
2. See Nicolo, G.; P. Bartholomew; J. Zaman and M. Zephirin, (2003).
3. The FSAP process is detailed in The Financial Sector Assessment Program, Factsheet, (Washington, D.C.: IMF, last updated September 24, 2013), Available at: <http://www.imf.org/external/np/exr/facts/fsap.htm> - "FSAP assessments are the joint responsibility of the IMF and World Bank in developing and emerging market countries and of the Fund alone in advanced economies, and include two major components: a financial stability assessment, which is the responsibility of the Fund and, in developing and emerging countries, a financial development assessment, the responsibility of the World Bank." With respect to assessing financial sector stability, "FSAP teams examine the soundness of the banking and other financial sectors; conduct stress tests; rate the quality of bank, insurance, and financial market supervision against accepted international standards; and evaluate the ability of supervisors, policymakers, and financial safety nets to respond effectively in case of systemic stress. While FSAPs do not evaluate the health of individual financial institutions and cannot predict or prevent financial crises, they identify the main vulnerabilities that could trigger one."
4. The laws contained in Sections 23A and 23B of the Federal Reserve Act are codified at Chapter 12, United States Code (U.S.C.) Sections 371c and 371c-1, respectively.
5. See Basel Committee on Banking Supervision, (1975) and Basel Committee on Banking Supervision, (1983).
6. See Bank for International Settlements, (1979).
7. See Basel Committee on Banking Supervision, (2012).
8. Specifically: CP 1 – arrangements for sharing information between supervisors and protecting the confidentiality of information should be in place; CP 3 – the prior consent of home country supervisors should be obtained prior to licensing foreign banks; CP 5 – ensure that corporate affiliations or structures do not expose the bank to undue risks or hinder effective supervision; CP 10 – loans to related companies must be on an arm's-length basis; CP 18 – bank prudential returns and statistical reports should be on a solo and consolidated basis; CP 23

– banking supervisors must practice global consolidated supervision over their internationally-active banks, adequately monitoring and applying appropriate prudential norms to all aspects of the business conducted by these banks worldwide, primarily at their foreign branches, joint ventures and subsidiaries; CP 24 – a key component of consolidated supervision is establishing contact and information exchange with the various other supervisors involved, primarily host country supervisory authorities; and, CP 25 – banking supervisors must require local operations of foreign banks to be conducted to the same high standards as are required of domestic institutions and must have powers to share information needed by the home country supervisors of those banks for the purpose of carrying out consolidated supervision.

9. See Basel Committee on Banking Supervision, (2012).
10. See Basel Committee on Banking Supervision, (2012).
11. See “Principle 12: Consolidated Supervision” and “Principle 13: Home-host Relationships,” In Basel Committee on Banking Supervision, (2012), pp. 35-39.
12. Basel Committee on Banking Supervision, (1999), p. 53: “A ‘noncompliant’ assessment is given when no substantive progress towards compliance has been achieved.”
13. “Implementation of the Basel Core Principles for Effective Banking Supervision,” International Monetary Fund, Washington, D.C., 2 September 2008, p. 12.
14. Assessed countries were Austria, Barbados, Canada, El Salvador, Italy and Singapore.
15. The 2012 BCP describe, in pertinent part, “compliant” grades as follows: “Compliant – A country will be considered compliant with a Principle when all essential criteria applicable for this country are met without any significant deficiencies”; “Largely Compliant – A country will be considered largely compliant with a Principle when only minor shortcomings are observed that do not raise any concerns about the authority’s ability and clear intent to achieve full compliance with the Principle within a prescribed period of time. (This grade)...can be used when the system does not meet all essential criteria, but the overall effectiveness is sufficiently good, and no material risks are left unaddressed.”
16. In the Keynote Address to the 10th Asia-Pacific High-Level Meeting on Banking Supervision, Stefan Ingves, Chairman of the Bank for International Settlements, described banks as being highly leveraged firms. Also see Bank for International Settlements, (2013).
17. See “IV. Capital Adequacy and Liquidity,” In Joint Forum, (2012), pp. 25-31.

18. See paragraphs 20-23 of the Basel Committee on Banking Supervision, (2006).
19. On 31 May 2012, in “Turmoil Frays Ties Across Continent,” the Wall Street Journal reported that UniCredit had transferred of €11.3 billion from its German subsidiary to alleviate funding difficulties faced by its Italian operations.
20. Extracted and amended from the 2013 Global Survey conducted by the Institute of International Bankers.
21. See “Principle 12: Consolidated Supervision,” in Basel Committee on Banking Supervision, (2012), pp. 35-37.
22. The Basel Committee notes “the importance of parent companies and other non-banking group entities in any assessment of the risks run by a bank or banking group [...] supervisory ‘risk perimeter’ extends beyond accounting consolidation concepts.” See paragraph 22 of Basel Committee on Banking Supervision, (2012), p. 6.
23. See Financial Stability Board, (2011).
24. See Financial Stability Board, (2013).
25. See “II. Supervisory Responsibility,” in Joint Forum, (2012), p. 12-17.
26. See HM Treasury, (2010).
27. See Zeti Akhtar Aziz, (2013) for further elaboration on the importance of cooperation and coordination arrangements across borders and its associated challenges.
28. Paragraph 23 of the BCBS’s Basel II (Risk-Weighted Assets) framework highlights that “... one of the principal objectives of supervision is the protection of depositors... supervisors should test that individual banks are adequately capitalized on a stand-alone basis” (p. 7). Similarly, essential criteria No. 7 of BCP 12 of the Basel Committee’s Core Principles of Effective Banking Supervision highlights that in addition to consolidated supervision, “the responsible supervisor supervises individual banks in one group. The responsible supervisor supervises each bank on a stand-alone basis and understands its relationship with other members of the group” (p. 37).
29. See paragraph 77 of Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms.

30. As stated in the Basel Committee's Regulatory Consistency Assessment Programme (RCAP) Assessment of Basel III Regulations in Brazil. See Basel Committee on Banking Supervision, (2013), p.18.
31. The European Union, for example, has proposed a common framework of rules for protecting deposits and for dealing with banks in difficulty across the European Union's single market. Within Asia, a number of central banks and monetary authorities have also established cross-border collateral arrangements aimed at enhancing the availability of liquidity facilities to regionally-active financial institutions operating in multiple jurisdictions.
32. Some jurisdictions have proposed or developed measures to insulate depositors or certain types of financial activities deemed as critical for the real economy from the risks that emanate from less critical activities which may pose a higher risk. See Gambacorta and van Rixtel, (2013).

References

- Bank for International Settlements, (1979), Consolidated Supervision of Banks' International Activities, March.
- Basel Committee on Banking Supervision, (2012), Core Principles for Effective Banking Supervision, September.
- Basel Committee on Banking Supervision, (1999), Core Principles Methodology, October.
- Basel Committee on Banking Supervision, (2006), International Convergence of Capital Measurement and Capital Standards, June.
- Basel Committee on Banking Supervision, (1983), Principles for the Supervision of Banks' Foreign Establishments, May.
- Basel Committee on Banking Supervision, (2013), Regulatory Consistency Assessment Programme (RCAP) Assessment of Basel III Regulations in Brazil, December.
- Basel Committee on Banking Supervision, (1975), Report on the Supervision of Banks' Foreign Establishments – Concordat, September.
- Financial Stability Board, (2011), Key Attributes of Effective Resolution Regimes for Financial Institutions, October.
- Financial Stability Board, (2013), Recovery and Resolution Planning for Systemically Important Financial Institutions: Guidance on Developing Effective Resolution Strategies, July.
- Gambacorta and van Rixtel, (2013), "Structural Bank Regulation Initiatives: Approaches and Implications," *BIS Working Paper*.
- HM Treasury, (2010), A New Approach to Financial Regulation: Judgment, Focus and Stability, July.
- Joint Forum, (2012), Principles for the Supervision of Financial Conglomerates, September.
- Nicolo, G.; P. Bartholomew; J. Zaman and M. Zephirin, (2003), "Bank Consolidation, Internationalization, and Conglomeration: Trends and Implications for Financial Risk," *IMF Working Paper*, 03/158.
- Zeti Akhtar Aziz, (2013), "The Central Bank Financial Stability Mandate and Governance Challenges," *SEACEN Financial Stability Journal*, Volume 1.



©2014 The SEACEN Centre

Published twice a year by:
The South East Asian Central Banks (SEACEN)
Research and Training Centre
Level 5, Sasana Kijang, Bank Negara Malaysia
No. 2, Jalan Dato' Onn
50480 Kuala Lumpur
Malaysia

Tel: 603-9195 1888
Fax: 603-9195 1801 / 1802 / 1803

*All rights reserved.
No part of this publication may be reproduced, stored in a
retrieval system, or transmitted in any form by any system,
electronic, mechanical, photocopying, recording or
otherwise, without prior permission of the copyright
holder, The SEACEN Centre. Please contact the
Communications Unit of The SEACEN Centre of the
above address to request permission.*



The **SEACEN** Centre

The South East Asian Central Banks (SEACEN)
Research and Training Centre

www.seacn.org