Bandid Nijathaworn: Meeting security and risk challenges in the finance and infrastructure sectors

Opening address by Dr Bandid Nijathaworn, Deputy Governor of the Bank of Thailand, at the seminar on “Meeting Security and Risk Challenges in the Finance and Infrastructure Sectors”, Bangkok, 11 February 2008.

* * *

Distinguished guests

Ladies and gentlemen,

It is a great pleasure to be here this morning, to give this opening remark for the seminar on “Meeting Security and Risk Challenges in the Finance and Infrastructure Sectors”. And those of you who come from abroad to join the seminar, let me also welcome you to Bangkok.

Today, risk management and security concern are important management issues for all businesses, as companies increasingly operate in an evolving global environment of rapid technological change and innovation.

Great advance in information technology has brought about radical changes in the way modern businesses are conducted and managed, and in the way new products and delivery channels are created. Yet while these changes have imparted important benefits to businesses in terms of profitability and efficiency, they also pose greater challenge in terms of the risk exposure and the management of risks. In this regard, I think financial services and banking is of no exception. It is one industry that continues to face this important challenge.

Banking business, basically, is about risk-taking, managing risk and profiting from risk. The growing sophistication and complexity of financial activities, brought on by financial innovation and globalisation, have made risk management a key and important task for all banks.

In particular, the integrity of real-time information on changing prices, valuation of financial position, and warning on breaches of internal control is most critical now for bank’s top management in taking timely and prudent decision. The recent episode in the global financial market has demonstrated again the costly implication of weaknesses in this area.

For these reasons, information technology and its management has become a key part in business strategy as it can provide lever to create competitive edge and innovate business model, especially for providing customer reach in a cost-effective manner. But on top of this, pressure from competition and the need to cut costs also have forced banks to rethink their business models and strategies, leading to fundamental changes in the business process that include the proliferation of outsourcing, electronic banking, and the use of the internet. Again, while these developments are positive, they also expose banks to a different aspect of risk management, for example how to manage and control outsourced activities. Such an environment, if not properly managed, can lead to greater technological and security risk, as well as to malicious activities.

For central banks, one of our key mandates is to ensure financial system stability. A key part of this is to make certain that banks and financial markets perform their functions efficiently, and that their business poses no systemic threat to the financial sector and the economy.

Hence, for a long time now, the main focus of bank regulation and supervision have been to ensure that banks manage their exposure to risk effectively. These include exposure to credit risk, market risk, liquidity risk, and operational risk. Much progress has been made in honing the approach for a more accurate assessment and a more effective management of risk, culminating in the Basle II, which is a global standard for bank’s risk management.

But, in spite of what has been achieved, mishaps can and do happen. From time to time, we still read about banks suffering large losses that originate from the under-management of these risks. More often than not, the losses are linked to a breach of internal controls or systems that have been put in place to rein in excessive risk-taking in the first place.

Ladies and gentlemen.

On the security risk aspect, the growth of electronic banking and real-time funds transfer have made the challenge of risk management even greater, as the nature of security risk to banks has shifted considerably. Clearly, the main concern now is not so much about ensuring property security or preventing theft of physical assets, but about ensuring information security and preventing identity theft. The concern is not so much about control over access to restricted areas and cash vault, but about ensuring proper authorized access to the IT systems and the electronic funds transfer network. And the issue is not so much about keeping bank premises open after a major disaster, but about ensuring that all key banking operations and network continue to function uninterrupted under a proper business continuity plan.

These are aspects of modern security risks to banks. They are part of the broader operational risks, which have received greater attention as the business of banking moves further and further away from face-to-face transactions. In Thailand, to address this challenge, we as bank supervisors, have over the past years provided best-practice guidance to the local banking industry in a number of important areas, including loss data collection, business continuity management and plan, IT security, outsourcing, and IT disaster recovery.

In addition, Basel II will, for the first time, impose an explicit capital charge on banks for operational risks, on top of the traditional credit and market risks. Implementation of Basel II in Thailand will begin at the end of this year, and the preparation for its implementation is progressing on schedule. I am confident that with the implementation of Basel II, the quality of risk management by banks in Thailand, especially with respect to operational risks, will improve further.

I have taken a lot of your time in this opening remark. But the topic of today's seminar is important. So, without further ado, may I declare the seminar open and wish you all a successful deliberation over the next two days. Thank you again for the invitation, and thank you for your attention.