Tarisa Watanagase: Supervisory concerns in an IT environment

Speech by Dr Tarisa Watanagase, Deputy Governor of the Bank of Thailand, at the 2nd SEACEN/ Federal Reserve System Course on Electronic Banking and Technology Risk Supervision, Bangkok, 12 May 2005.

* * *

Financial institutions increasingly rely on technology to do their businesses, as a result, improper management and operation of IT will bring risks to financial institutions. Also, issues associated with IT including technological changes, new threats and vulnerabilities will no doubt affect financial institutions' performance and risk profile. Therefore, it is necessary to integrate IT risks with risk-based supervision in order to obtain a comprehensive risk profile of a financial institution. Today is a good opportunity for me to share with you our thoughts and experiences on Supervisory Concerns in an IT Environment.

1. Overview of current IT environment in the banking sector

- The Thai financial institutions have been using IT in their businesses for decades. Initially, IT was used as a supporting tool for banking operations, helping staff do their work faster, more conveniently and with less human errors. Then, along with more advanced technology, many financial institutions now offer their products and services through electronic channels such as internet banking, mobile banking, ATM, etc. These alternative banking channels provide customers much easier and more time-saving ways to do their transactions with banks.
- In addition to offering alternative banking channels, financial institutions currently also take advantage of IT to innovate financial products and services. For example, through system-integrated capability, financial institutions can offer a wider range of services including bill payment and tax payment. Electronic money (E-money) is a new product that is now offered by many institutions, both banks and non-banks. All of the aforementioned products and services delivered with the help of IT and the effort on core-banking system integration require much more complex technology infrastructure which raises tendency to the use of IT Outsourcing services from external expertise. As a consequence, financial institutions can fully focus on core activities and become less concerned with not having a sophisticated level of IT expertise. However, financial institutions must be aware that risks from outsourced operations still fall under their responsibility even though they may not undertake IT operations by themselves.
- As the use of IT becomes widespread, it appears that most Thai financial institutions are adopting international best practices as a framework to create a controlled environment and manage risks that might occur from IT related operations. As new security threats emerge, it becomes necessary to have adequate control mechanism to protect banks' information assets including hardware, software and data.
- As we all know, after 9/11, this issue has become a global concern. Most financial institutions are aware of the need to have Business Continuity Management. The business continuity plan has to be established on an enterprise-wide basis with a thorough business impact analysis and risk assessment. It is more than just the recovery of technology; it is the recovery and continuity of business.
- With the widespread use of IT, it is important that the legal framework is in line with the new environment. Thailand has started to legislate five new Information and Communication Technology (ICT) Laws to embrace information technology since 1998. They are the Electronic Transactions Law, Computer Crime Law, Data Protection Law, Electronic Funds Transfer Law, and the National Information Infrastructure Law. The Cabinet has appointed the National Electronics and Computer Technology Center (NECTEC) to take charge of the drafting of these laws. The Electronic Transactions Law was promulgated on April 3, 2002 while the others arc in the process of enactment.

2. E- banking products in Thailand and supervisory concerns

What I would like to do next is to give you some examples of IT-related financial products and services currently offered in Thailand and the pertinent risk issues that bring up supervisory concerns. Let me start by briefly showing you our data on e-banking service usage by category.

In the first four rows of the table, the figures show customers' e-banking transactions that have high transaction volumes but low average values.

In the remaining rows, you will find that the Bank of Thailand is the sole service provider facilitating wholesale payment transactions between financial institutions and the central bank. Even the number of transaction is much smaller, the value is certainly much higher. This type of transaction of course has different risk implications from that with higher transaction volume in smaller amount of money.

Internet banking in Thailand can be classified into two categories, **informational and transactional websites**. The **informational website** provides banking information including products, services, interest rate, foreign exchange rate, etc. On the other hand, the **transactional website** is a channel for customer transactions such as money transfers and bill payments as well as inquiries such as balance inquiries and statement download.

Since internet is ubiquitous and global in nature, it is an open network accessible from unknown sources. Messages are routed through unknown locations. Therefore, internet significantly magnifies the importance of **security control and protection against fraud, hacking and other possible internet security threats**. A financial institution needs to have a strong authentication process to prove the identity of the person who logs onto the service before any transaction is allowed. Since transaction via internet does not require face-to-face contacts, non-repudiation becomes another major issue as the ability to prove that a customer did request a transaction on service. As supervisors, we need to encourage FIs to implement strong security and control measures as well as provide mechanisms to keep abreast with emerging threats.

E-Money, or known otherwise as Multipurpose Stored Value Card, E-Purse, E-Wallet, or Smart Card has three major characteristics.

1. **Pre -paid**: Consumer pay money in advance to e-money issuer.
2. **Store value**: Amounts of advance are stored in electronic media such as plastic card.
3. **Multipurpose**: Consumer can use money paid in advance to purchase goods and services from different retailers determined by the e-money issuers

E-money can be categorized into network-based and card-based depending on how the value is stored.

- **Storing value in a network basis** requires no physical item to store value but is kept in the service providers' system.
- **Storing value in a card-basis is the** use of a plastic card with embedded chip to store value.

E-money is regarded as **non-traditional financial services which lead to new ways of security and control implementation**. Furthermore, it may facilitate **money laundering activities**. That is why in Thailand, we prohibited the transfer money among customers without going through service providers' data system. In addition, the system must be able to trace all activities. A bank should set a maximum limit of e-money that can be used . And, it can only be issued in Thai Baht currency and used in Thailand.

IT outsourcing means allowing other service providers to perform on behave of a financial institution IT functions which are normally done by the institution itself. By the advent of rapid changes in technology and competition, financial institutions tend to reduce costs and to improve their services by outsourcing some technology-related functions to third parties both within and across borders. In Thailand, we see a few distinctive characteristics of IT outsourcing services.

- **Full scope of IT operations**. This is to outsource the entire IT resources and operations including location, equipment, hardware, software, staff, facilities, communication and other necessities to the third-party service providers. By that, financial institutions will not involve in those operations but rather assign a coordinator to monitor the performance of the provider.

- **Selective areas of IT operations**. With this, a financial institution may acquire a certain service of a provider, for example, renting the facility of a service provider to operate its back-up hardware and software.

Both full and selective scopes of outsourcing can be carried out with a third-party service provider residing domestically or abroad. This raises supervisory concerns. Since financial institutions' data including customer and transaction data are processed by other parties, A financial institution must ensure its **data integrity, security and confidentiality** to prevent data leakage and mishandling. Moreover, though operated elsewhere - whether domestically or abroad, **system reliability and availability** still fall under the financial institutions' responsibilities. All of these issues can in fact impact the institution's reputation, image and credibility.

E-banking frauds in Thailand

E-banking, unfortunately, also brings about electronic frauds. There are two major kinds of frauds thriving in electronic payment environments in Thailand: card-based and networks-based frauds.

Card-based frauds include counterfeited ATM and Credit cards, and **Skimming**, which involves copying the magnetic stripe encoding from debit or credit cards to forged cards The network-based fraud is called "**Phishing**". This is an identity theft whereby Internet hackers trick some naïve customers into revealing their sensitive information such as User ID and password through fake email addresses, through social engineering, or spy ware. The Bank of Thailand has recently issued notifications to address these issues and encourage financial institutions to raise customer awareness of such frauds through education.

As stated earlier, financial institutions now take advantage of IT to innovate financial products and services. **Such innovation brings to a financial institution new dimensions to traditional risks**, which include strategic risk, credit risk, market risk, liquidity risk and operational risk. Therefore, the lack of efficient and appropriate controls may amplify the likelihood of each risk and its impact. Internet banking, e-money and IT outsourcing are good examples that highlight the importance of IT supervision. At this point, may I draw your attention to the next topic which is IT risk-based supervision.

3. IT risk-based supervision

BOT has adopted risk based supervision for the past several years.

Supervision objectives:

The primary objective of BOT supervision is to encourage FIs in Thailand to conduct banking business in a **safe and sound manner** and **consistent with related laws, rules and regulations**. It is also our duties to ensure that supervisory framework is keeping up with demand from the financial community as well as with **market innovation, international best/ sound practice**; finally, to protect **customer rights as well**.

IT risk-based supervision helps ensure the safety and soundness as well as legal compliance of a FI. As already mentioned, IT does not trigger new type of risks but brings in new dimensions to traditional banking risks. At this point, I would like to first give you the definitions of risks directly associated with IT. May I begin with strategic risk.

Scope of IT risk-based supervision:

1. Strategic risk

Strategic risk **arises from adverse business decisions or improper implementation of those decisions**. Use of technology can create strategic risk when management does not adequately plan for, manage, and monitor the performance of technology-related products, services, processes, and delivery channels.

2. Operational risk

Operational risk is **the risk in the areas of security, data confidentiality, data and system integrity, and outsourcing causing problems with product and service delivery**. This type of risk often results from failure to establish adequate security measures, contingency plans, testing, and auditing standards. Operational risk can increase when a financial institution hires outside service providers to design products, services, delivery channels, and processes that do not fit with the financial institution's systems or customer demands. Deficiencies in system design, implementation, or maintenance of systems or equipment also tamper with data integrity.

The IT exposure usually does not limit to just these two risk types. Improper IT management and operation can lead to compliance risk and reputational risk.

3. Compliance risk

Compliance risk is arises **from violations of, or non-conformance with, laws, rules, regulations, or ethical standards**. Some new technologies raise unexpected compliance issues. For example, transactions conducted through the internet can also raise questions regarding jurisdictional authority over those transactions. Cross border activities raise a number of concerns to supervisors on how to supervise banking businesses with no physical presence in the country, and also how to effectively manage risks involved in cross-border transactions.

4. Reputational risk

Reputational risk **arises whenever technology-based banking products, services, delivery channels, or processes generate adverse public opinion**. For example, breaches of security and disruptions to the system's availability can damage financial institutions' reputation. Also, system disruptions or doubts about the integrity of the system or data could result in a loss of confidence in electronic delivery channels as a whole, and can potentially affect other e-banking providers.

IT risk-based supervision focuses on strategic and operational risks.

Strategic risk

Supervisory objective

In strategic risk supervision, supervisors have to ensure that Financial institutions have efficiently managed their IT resources and are prepared for the future development of core businesses.

Supervisory areas

Therefore, to achieve such objective, supervisors will assess risks that may arise in the following areas.

Policy perspectives

Since enterprise activities require information from IT to meet business objectives, effective IT strategic planning is mandatory. The strategic plan refers to how to utilize IT in an organization. IT must be aligned with and enable the enterprise to take full advantage of its information, thereby maximizing benefits, capitalizing on opportunities and gaining a competitive advantage. As such, IT policy, plan and procedure are the concentrated areas for supervisors to examine. We anticipate a financial institution's policy to cover all necessary areas pertaining to IT activities including contingency plan, security, and out/in-sourcing. In addition, the policy should cover new product issuance such as internet banking and e-money. The process of formulating, implementing and maintaining of such policies should be considered. A continuous risk assessment and monitoring should also be part of an area of examination.

Management support and oversight

It is ultimately a responsibility of a financial institution's board and management to extend governance to IT and provide the leadership, organizational structures and processes to direct and control the enterprise. Management must monitor to ensure that IT resources are properly managed to promote business objectives.

IT governance

During the last few years, financial institutions have increasingly invested in technology infrastructure to improve their internal processes and servicing capabilities. Investment in technology infrastructure normally involves huge amount of funds and other resources. Technology also carries risks, which can adversely affect financial institutions if not properly managed. Financial institutions need to understand the strategic importance of IT, manage IT to effectively deliver value to business, and mitigate risks arisen from the use of IT.

IT governance focuses on how financial institutions make the best use of their invested technologies. It is a high-level IT control framework related to the formulation of IT strategies, the management of IT processes to deliver value, the performance measurement, and the management of IT-related risks.

We believe that effective IT governance process will enable financial institutions to effectively utilize their technologies to meet business' expectations and to add value to their business. In that way, IT will truly help the organizations to improve competitive advantage, customer satisfaction, cost efficiency, and ability to grow and innovate the business. Eventually, it will help financial institutions to realize better return on investment in technology infrastructure.

Independent audit and review

A financial institution is required to have IT independent audit and review all IT related areas to ensure that the board and management emphasize IT as a key business driver. IT controls are evaluated and those having a material impact on financial processes are specially focused. The assessment of these controls should be conducted on a regular basis. In Thailand, we require financial institutions to perform IT audit at least once a year. In addition, we also require an independent assessment of internet security.

Now, let's turn to operational risk.

Operational risk

Supervisory objective

In operational risk supervision, supervisors have to ensure that financial institutions have adequate security measures, data integrity process and contingency plans in place.

Supervisory areas

The focal point when we evaluate operational risk regarding IT is to ensure a financial institution establish adequate control mechanisms in IT process and procedure. The control can be done either technically or manually, or both. Segregation of duties is an example of manual control which should be maintained especially for critical functions or processes to prevent fraud. Additionally, controls should be embedded in the system to ensure integrity of input, processing and output. Adequate physical and logical access controls are important since they can protect data, system and resources from unauthorized persons. Finally, a financial institution should provide alternative resources for backup and recovery, and ensure that they can be available during an event of a disruption. All of these matters are about **security and confidentiality, integrity and availability** which will be elaborated more in the next slide.

Security and confidentiality

Supervisory objective

An objective of IT supervision in **security and confidentiality** areas is **to ensure of IT activities being conducted in a secure and control environment and of data confidentiality and integrity by laws, rules and regulations.**

Supervisory areas

To achieve such objectives, the following points should be addressed by supervisors.

Physical security: It is about **control for environmental exposures** due primarily to mother-nature events such as lightning, storms, flood and etc. Others may be caused by human acts such as

terrorist, fire, electronic shock and equipment failure. The result of such conditions can damage computer system, equipment and facilities which in turn cause an interruption. Another type of physical security is **physical access controls** which aim to prevent unauthorized access to computer system, equipment and facilities as well as data. Examples of this type of controls are electronic door locks, biometric door lock, video camera, etc.

Logical security: It is **data, system and network access control**. Lack of adequate logical security may be prone to technical exposure to unauthorized implementation or modification of data and program at either the network, platform, database or application level. A classic example of this type of controls is the use of user ID and password.

Supervisor should be able to analyze and evaluate the effectiveness of both physical and logical access control in accomplishing financial institution's information security objectives.

Integrity

Supervisory objective

An **objective** of IT supervision in an **integrity** area is **to ensure reliability and completeness of system functionality in order to verify that data is processed in an accurate and timely manner**.

Supervisory areas

Therefore, supervisors need to review and assess whether financial institutions have sound application control in place. In this regard, they should have control built in the procedure and programmed in the system to ensure the **integrity of input, process and output**. In a large financial institution using various applications, a sample of applications including core banking applications and management information system (MIS) would be examined for control adequacy. Data and system integrity can reflect the effectiveness of system development, acquisition and change control procedure. Therefore, it is necessary to cover those areas in the scope of supervision.

Availability

Supervisory objective

An **objective** of IT supervision in an **availability** area is **to ensure financial institutions' readiness for being able to run business without interruption during an occurrence of disruption**.

Supervisory areas

In this regard, supervisor must review and assess the **scope of business continuity plan** which should be established in an enterprise-wide basis. Also, the best way to determine how well the plan works or which portions of the plan need improvement is through **testing**. We encourage financial institutions to test the disaster recovery plan at least once a year. Finally, financial institutions should have a procedure in place to **update the plan regularly**.

4. IT examination and risk assessment

Objective

The objective of IT examination and risk assessment is **to assess a financial institution's IT management and operation to ensure accuracy and reliability of information system as well as its alignment with the financial institution's business objectives which can eventually bring in the safety and soundness**.

IT examination process

There are three main steps to be taken when performing IT examination.

1. Pre -examination

This step is the process of gathering the information about the financial institution on which we will conduct examination. The information including business nature, objective, policy, plan, IT infrastructure and organization chart can be obtained from **previous examination reports, internal database and external sources**. At this step, IT examiners will **coordinate with Onsite examiners** to share information and identify areas of concerns. With all of the gathered information, examiners can preliminarily assess IT role in supporting FI business and prepare scope of examination.

2. Onsite examination

The next step is to conduct onsite examination at a financial institution. Normally, IT and Financial or Safety and Soundness examinations are performed concurrently where their examination results are integrated together for an overall risk assessment. At this stage, examiners gather information through a variety of examination techniques such as interview, observation, review of documents to summarize the findings.

3. Post examination

After the findings, examiners will assess the risks of those findings and report on significant issues. **The risks regarding IT are assessed and assigned to IT risk rating which is divided into three levels, high, medium, low with respect to the probability of occurrence and the degree of impact to a financial institution. For significantly high risk issues which indicate serious control weaknesses which then need an immediate correction, we could** enforce the FI to take corrective action **within a predetermined period of time. And, it is our duty to monitor compliance with such an enforcement action. This is a process of** follow-up

The risk assessment is performed not only when conducting IT examination but also when considering new products and services' applications. **Currently, the products and services that need BOT's IT risk assessment prior to approval are internet banking and e-money.**

IT Risk Assessment Factors, at a minimum, include:

Security: The financial institutions have to prove that they have adequate security measures in place to ensure that information is protected against harm from threats leading to different types of vulnerabilities such as loss, inaccessibility, alteration or wrongful disclosure.

Risk management: Risks of new products and services must be thoroughly considered by the financial institution. There should be a policy and procedure in place to manage the risks.

Internal control: The financial institutions should set up preventive, detective and corrective control mechanisms that may be built in the operating procedure or programmed in the system involving new product and service delivery.

Contingency plan: The financial institutions should formulate the contingency plan to carry on the business under unexpected events.

Staff development: The financial institutions should establish a staff development plan to enhance personnel capabilities to conduct new product and service operations.

Last topic of presentation is new challenges for BOT supervision and ways to overcome.

5. New challenges for BOT's IT supervision and ways to overcome

(1) While the financial industry is moving fast with innovations and new developments, supervision needs to ensure the stability of the financial system. Supervisors need to encourage financial institutions to operate their businesses in a safe and sound manner as new delivery channels or services could exacerbate some of the same risks inherent in traditional banking.

However, the prudential regulatory framework has to be congruent to the evolution of the e-banking business. Therefore, we need to **strike a balance between the need to maintain the stability of the financial system and to foster developments, competition, and a level playing field**.

There are ways to overcome this challenge.

- Regulators need to keep up with the development of the market while being proactive in formulating the regulatory framework. In the case of Thailand, BOT takes an active role in **meeting regularly with financial institutions and IT companies** to exchange views and experiences on the development of the businesses and IT environment.
- In the process of drafting policies, we often **seek out the view from our fellow regulators** to ensure that our policy are in line with market and **international practices**, as well as to help us anticipate problems that may arise in implementation.
- The final drafts of policies are sent out for **comments** from key stakeholders in and outside the Bank of Thailand, especially the industry, to ensure that the policies are practical and not posing any undue burden on financial institutions.
- We also make sure that **revision of regulations and guidelines** is conducted regularly to ensure that e-banking policies are keeping with demand from the financial community as well as with market innovation and international best practices.
- To maintain **proactive supervision**, the IT **risk-based supervision is conducted continuously**, updating each of bank's IT risk profile on a regular basis and performed overall assessment in certain areas. In case of getting a report of any incidents, we have to thoroughly analyze the impact on the financial institution system and consumer. And, to prevent recurrence of such incidents, we may urgently **issue notification to financial institutions to provide preventive, detective and corrective control measures** in self and customer protections.

(2) With the rapid development in technology, in the near future, apart from the known internet banking, we will see more of the "non-traditional" banking products. The providers of these services will not only be limited to banks, but also non-banks. Of course, the extent to which a non-bank provider can offer these new products and services depends on the rules and regulations of each country. To promote a fair competition between service providers that are banks and non-banks is a challenge for the authorities.

BOT is in course of shifting from supervision by institutional basis to transactional basis which will enable us to overcome such a challenge.

(3) After the financial crisis, the need for strengthening supervision of financial institutions has been stressed as a major priority to BOT. The monitoring of financial institution systems becomes both more critical and more challenging for supervisors. The "Core Principles for Effective Banking Supervision" have become the most important global standard for prudential regulation and supervision. They are developed by the Basel Committee on Banking Supervision in cooperation with supervisors from noiQ-10 countries, providing the international financial community with a benchmark against which the effectiveness of bank supervisory regimes can be assessed. IT supervision is also included in the Core Principles such as CP9 (MIS), CP 11 (Information System to comply with Country Risk and Transfer Risk), CP13 (Contingency Plan, MIS, Business Resumption Plan) and CP21 (verification of information from bank records by on-site examination and/ or external audits). Therefore, **How to achieve full compliance with the Core Principles becomes another challenge for BOT supervision.**

The BOT, with the assistance of the IMF and the World Bank, has finished our self-assessment of our compliance with the Principles. Weaknesses in the existing system of supervision and regulation have been identified, and will form a basis for future remedial measures.

The other two challenges involve the creation of internal expertise for IT supervision in order to be more responsive with technological evolution.

The first is **to enhance supervisors' technical know-how**. The way to overcome this challenge is to **provide regular training** to supervisors. Some in-depth technological knowledge is necessary. The supervisors should be given tools to **keep up with new technology, vulnerability, threats and other forces. Research and development** for IT supervisors should be considered.

Another challenge is to **formulate policy with flexibility, forward-looking and reflecting changing business nature**. One way to overcome this challenge is to **broaden the view and knowledge of supervisors** which can be accomplished by all aforementioned matters.

6. Conclusion

In conclusion, technology is still changing and financial institutions tend to depend more on it. BOT has no intention to interfere with financial institutions' innovation; however, while technology is becoming more and more complex, so are the threats. A financial institution needs to have active IT management to provide secure and reliable services to customer. Supervisors need to keep updates with those new issues. In addition, it's not only a supervisor's job to maintain the stability of banking industry but also banker's. Both sides should put efforts together to create a safe and sound environment and should always recognize the significance and effects of technology towards the banking industry. So, **working in a proactive and more collaborative manner is the solution for today's supervisors'.**