THE SUPERVISORY IMPACT OF TECHNOLOGY ON SEACEN FINANCIAL INSTITUTIONS: ISSUES AND CHALLENGES

Cicilia A. Harun

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

Published by The South East Asian Central Banks (SEACEN)
Research and Training Centre
Lorong Universiti A
59100 Kuala Lumpur
Malaysia

Tel. No.: (603) 7958-5600
Fax No.: (603) 7957-4616
Telex: MA 30201
Cable: SEACEN Kuala Lumpur
Website: http://www.seacen.org

THE SUPERVISORY IMPACT OF TECHNOLOGY ON SEACEN FINANCIAL INSTITUTIONS: ISSUES AND CHALLENGES

ISBN: 983-9478-71-0

Printed in Malaysia by:

Attin Press Sdn. Bhd.
No. 46, Jalan 3/108, Taman Salak Jaya,
Salak Selatan, 57100 Kuala Lumpur.
Tel: 03-7984 7626
Faks: 03-7981 5253

TABLE OF CONTENTS

PART 2: COUNTRY CHAPTERS

CHAPTER 2 :THE SUPERVISORY IMPACT OF TECHNOLOGY ON SEACEN FINANCIAL INSTITUTIONS: ISSUES AND CHALLENGES IN BRUNEI DARUSSALAM

by Zaki Mohidin

CHAPTER 3: THE SUPERVISORY IMPACT OF TECHNOLOGY ON SEACEN FINANCIAL INSTITUTIONS: ISSUES AND CHALLENGES IN CAMBODIA

by Hay Livine / Sim Sothearith

CHAPTER 4: THE SUPERVISORY IMPACT OF TECHNOLOGY ON SEACEN FINANCIAL INSTITUTIONS: ISSUES AND CHALLENGES IN INDONESIA

by Cicilia A. Harun

CHAPTER 7: THE SUPERVISORY IMPACT OF TECHNOLOGY ON SEACEN FINANCIAL INSTITUTIONS: ISSUES AND CHALLENGES IN NEPAL

by Shiba Raj Shrestha

FOREWORD

Given the increasing intensity of IT implementation by financial institutions in most of the SEACEN member countries, this project is considered timely to address the relevant issues and challenges faced by all SEACEN member countries. The objective of the project is to identify concerns in the IT practices of financial institutions in the region, emphasising on the practices by banking institutions. The level of IT implementation by financial institutions in the region varies from country to country. The research project addresses the most common concerns, elaborates on the different conditions and suggests policy measures to mitigate IT risks and finally, to highlight IT practices by financial institutions in the region to level the playing field.

This research project on ***The Supervisory Impact of Technology Implementation on SEACEN Financial Institutions: Issues and Challenges*** is a collaborative effort by The SEACEN Centre and a team of ten country researchers representing nine SEACEN member central banks, namely, Ministry of Finance of Brunei Darussalam, National Bank of Cambodia, Bank Indonesia, The Bank of Mongolia, Central Bank of Myanmar, Nepal Rastra Bank, Central Bank of Sri Lanka, Central Bank of the Republic of China (Taiwan) and State Bank of Vietnam. Reserve Bank of Fiji, Bank Negara Malaysia, Bangko Sentral ng Pilipinas, Monetary Authority of Singapore, and Bank of Thailand contributed input in form of responses to the survey questionnaire. The heterogeneity of IT implementation by financial institutions in the region is reflected in the country papers authored by the country researchers. This suggests that there need to be careful policy prescriptions in enforcing IT standards in the region. The integrative report provides the common thread that will lead to the overall conditions in the region. The research project does not attempt to provide a binding standardisation of IT implementation by financial institutions in the region. However, it addresses the issues and challenges in the provision of IT infrastructure and the design of IT supervisory framework to mitigate the potential problems involving the IT implementation. The international standards and best practices described in the integrative report as well as the practices in some of the more advanced countries in the region can be a yard stick for SEACEN member countries to improve on

their IT supervisory practices in order to bring IT implementation by SEACEN financial institutions to international standards.

The study is divided into two parts. Part I is the integrative report authored by Dr. Cicilia A. Harun, Visiting Research Economist at The SEACEN Centre who is currently a researcher at the Financial System Stability Bureau, Directorate of Banking Research and Regulations at Bank Indonesia. Dr. Harun served as the Project Leader as well as Country Researcher for Indonesia. Part II consists of nine country papers written by the country researchers from the nine members of SEACEN countries participating in the project.

The SEACEN Centre wishes to thank Dr. Harun for her efforts as the Project Leader and Country Researcher and also the Country Researchers from the participating SEACEN member central banks for their contributions to the research project, namely, Mr. Mohd. Khairul Zaki Hj Mohidin, System Analyst, Information Technology and State Store Department, Ministy of Finance, Brunei Darussalam; Mrs. Hay Livine and Mr. Sim Sothearith, both Section Chiefs of Economic Research Department, National Bank of Cambodia; Mrs. Tsolmon Baasanjav, Supervisor, Supervision Department, The Bank of Mongolia; Daw Khin Cho Cho, Assistant Director, Bank Supervision Department, Central Bank of Myanmar; Mr. Shiba Raj Shrestha, Director, Financial Institution Supervision Department, Nepal Rastra Bank; Mr. G K K Gamage, Senior Assistant Director, Bank Supervision Department, Central Bank of Sri Lanka; Mr. Lee Yi Chang, Senior Auditor, Department of Financial Inspection, Central Bank of the Republic of China (Taiwan) and Mr. Phan Thai Dung, Chief of Division, Informatics Technology Department, State Bank of Vietnam. The Centre also gratefully acknowledges the valuable comments and suggestions of Dr. Haibin Zhu, Senior Economist, Representative Office for Asia and the Pacific, Bank for International Settlements, on the final draft of this study.

The Centre also wishes to acknowledge the support of The SEACEN Centre's staff in completing this study. The views, conclusions and recommendations expressed in this Report are those of the authors and do not necessarily reflect those of The SEACEN Centre or its member central banks/monetary authorities.

Dr. A.G. Karunasena
Executive Director
The SEACEN Centre
June 2009

Executive Summary

The development of financial markets cannot be isolated from the influence of technology. Technology, especially information technology (IT), plays a dual role in the financial field - as the engine of development of financial products and as the engine of financial institution operations. The operations of financial institutions in SEACEN countries involving the use of IT take on the second role. The more advanced SEACEN countries can actually compete with the world leaders in IT implementation by financial institutions. However, in terms of the second role of IT, SEACEN countries are still following the lead of the developed countries.

This research project is aimed at providing a comparative study on the IT implementation within SEACEN financial sectors, including its supervisory impacts, issues and challenges. The project also serves as a documentation of the development of IT implementation by financial institutions in the SEACEN region. Since most central banks in the region are the authorities for the supervision of banking systems and not of non-bank financial institutions, the discussions on financial institutions pertain to banks. The project addresses the international best practices in IT implementation, cross-country comparison regarding IT implementation by financial institutions, the supervisory impacts, and the IT supervisory framework.

SEACEN countries have different levels of IT implementation and IT supervisory frameworks. The country papers and survey results show that there are three different levels of IT implementation in the SEACEN countries. They are: 1) Developed IT implementation and established IT supervisory framework; 2) Early stage of IT implementation with less-established IT supervisory framework; and 3) Less-developed IT implementation. For each level of implementation, countries face different issues and challenges. Wherever IT implementation has become an important part of financial institution operations and management, the SEACEN member central banks consider IT supervision as an integral part of the overall financial institution supervisory framework. However, since there is cross-country heterogeneity of IT implementation and IT supervisory framework, suggesting a minimum requirement for IT implementation for institutions and a model IT supervisory framework is very difficult.

The research project also addresses some issues and challenges faced by the countries in the region in terms of mitigating IT risks and bringing IT implementation by financial institutions in the region to a level playing field according to international best practices. The issues and challenges suggest the need to increase cooperation among the SEACEN member countries to increase IT awareness, implement good IT governance through establishing IT supervisory frameworks which conform to international best practices, increase knowledge sharing and training programmes in order to speed up the spill-over effects from the more advanced countries in the region.

PART 1: INTEGRATIVE REPORT

CHAPTER 1

THE SUPERVISORY IMPACT OF IT IMPLEMENTATION ON SEACEN FINANCIAL INSTITUTIONS: ISSUES AND CHALLENGES

by Cicilia A. Harun[1†]

1. Introduction

> *"A number of global forces have gradually, sometimes almost clandestinely, altered the world as we know it. The most visible to most of us has been the increasing transformation of everyday life by cell phones, personal computer, email, BlackBerries, and the Internet. ..... These new technologies not only opened up a whole new vista of low-cost communications but also facilitated major advances in finance that greatly enhanced our ability to direct scarce savings into productive capital investments, a critical enabler of rapidly expanding globalization and prosperity." (Alan Greenspan, "The Age of Turbulence" [Greenspan 2007])*

Technology has been a major part of the development of financial markets. The use of technology has broadened and deepened the financial sector. Financial institutions implement technology to reduce the costs of operation as well as to provide better services. Financial engineers exploit the speed and accuracy of computer technology to innovate new financial products. Technology has a dual role in the development of finance: as the engine of development of financial products and as the engine of the financial institution operation.

For the first role, technology has been the necessary tool to create products ranging from depository products with complex automatic options to derivatives, securities, and structured products. Financial engineers or product and services officers rely on the availability and the accuracy of computer systems to provide tailor-made financial products suitable for the demographics of the clients and customers. The use of information technology (IT) also offers abundant resources for knowledge sharing and research, reducing the cost of research and development for the innovation of products and services.

1 † Project Leader and Visiting Research Economist of The SEACEN Centre. She is currently Researcher at Financial System Stability Bureau, Directorate of Banking Research and Regulation, Bank Indonesia.

For the second role, technology has enhanced the payment system and accounting operation of financial institutions. Long-distance transactions now can be executed in a matter of seconds with the help of computer and communication technology. The use of information system also helps financial institution managers conduct better asset and liability management and offer better services to clients and customers. The everyday operation of financial institutions is nowadays largely dependent on the use of computer and communication technology.

Despite the requirement of high fixed cost for implementing it, IT has been a major part of the development of financial markets. Both institutional and individual players of the markets have benefited from the use of IT. The dual role of IT has provided mutual benefits in tapping customer preferences for marketing purpose, supported R&D to better manage investment and operations, and facilitated product differentiation that leads to larger captive markets and higher fee-based incomes.

Central banks –mostly authorities of the banking industry and sometimes authorities of non-bank financial institutions as well – place a lot of emphasis on the IT practices of financial institutions (FIs). Given the growing dependence of FIs on IT systems, IT risk has become an integral part of the overall operational risk. Modern central banks have started to incorporate IT audit in their supervisory framework. Bank supervisors with basic to high level of IT expertise are now in demand. Central banks (or banking supervisory authority) have begun to hire IT specialists/auditors to detect the possibility of high IT risk or IT fraud in a bank. In addition to reducing possible idiosyncratic shocks within individual banks, central banks – as payment system authority – also wish to ensure the reliability of the national payment system. Any possible disturbance from a member of the payment system can cause a large impact towards the overall operation of the payment system. Banks that have direct connection to the national payment system can be required to conform to the minimum system requirement and are obligated to have regular IT audit. Table 1.1 provides a brief description on the banking systems within the SEACEN member countries that are discussed in this research project.

Table 1.1

SEACEN Banking Systems

	Banking System Assets		Fraction of the Financial System+ (%)	Number of Banks
	In billions of local currency	In billions USD		
Brunei Darussalam	n/a	n/a	n/a	n/a
Cambodia -2007	13,445 (KHR)	3.36	n/a	17
Fiji- Dec 2007	3.9 (FJD)	2.50	50.90	5
Indonesia - July 2008	n/a	210	79.00	127
Malaysia - Nov 2008	1,247.37 (MYR)	36.61	n/a	39
Mongolia - July 2008	n/a	n/a	n/a	16
Myanmar	n/a	n/a	n/a	19
Nepal - August 2008	678,52 (NPR)	9.87	80.00	25
Philippines - May 2008	5,200 (PHP)	121.21	78.80	841**
Singapore-Nov 2008	657,21 (SGD)*	459.59		
Sri Lanka - Sept 2006	n/a	n/a	57.00	37
Republic of China (Taiwan) - June 2008	35,720 (TWD)	1,145.61	n/a	388
Thailand - June 2008	9,500 (THB)	286.58	n/a	34
Vietnam - June 2008	n/a	60	n/a	5***

\+ Financial system comprises the banking system and the non-bank financial systems

* Refers to Assets of Domestic Banking Units

** Refers to the number of head offices, comprising 38 universal and commercial banks, 80 thrift banks, and 723 rural and cooperative banks.

*** Refers to State Commercial Banks

Source : Country papers and survey responses for this research project.

Although the implementation of IT in the Asian countries came later than that of U.S. and Europe, Asian financial institutions are far from novices in using IT in their operations. In fact, some Asian countries are the leaders in term of adoption of IT in daily operations by financial institutions. This is in line with how well the Asians - especially in Japan, Hong Kong SAR, Korea, Singapore and other emerging markets in Asia - embrace the use of high technology in their everyday

lives[2]. The IT implementation by financial institutions in some of SEACEN member countries follows this trend in Asia. However, Asian countries are not the leaders in terms of having the international best practices of IT implementation. International best practices are mostly set up in the western developed countries. Because of this, the benefits and drawbacks of having sophisticated IT implementation in the financial institutions have to be assessed carefully. The investment spent on installing an IT system should be proportionate with the expense for mitigating the IT risks. The more dependent on its IT system, the more risk an institution will have to face, in association with the incidence of IT failure.

The U.S. and European countries have been developing standards for best practices in IT implementation. For one, ISO (headquartered in Geneva, Switzerland) has been issuing standards related with IT practices. The family of ISO27000 has been the most widely referred to by IT implementers in general. Second, Control Objectives for Information and related Technology or better known as COBIT is another set of standards for IT management created by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI) in 1992, both of which are U.S.-based. In addition, the Information Technology Infrastructure Library (ITIL) issues another set of concepts and policies for managing information technology (IT) infrastructure, development and operations. It even provides certification for companies conforming to the standards of ITIL. The ITIL is a registered trademark of the United Kingdom's Office of Government Commerce (OGC).

Especially for IT implementation by financial institutions, the U.S. established the Federal Financial Institution Examination Council (FFIEC). This is a formal interagency organisation that sets up standards for conducting IT supervision for financial institutions in the U.S. These standards are implemented within the banking supervisory framework of the Federal Reserve System. Within the Basel II framework, the Basel Committee on Banking Supervision (BCBS) has also established 14 principles for electronic banking (BCBS, 2003b). These principals are not meant to be standards of e-banking practices, but rather as guidance in the recognition of the risks related to e-banking activities and for overall risk management in a bank. In addition to that, there are many certification programmes to ensure IT professionals are qualified in performing their tasks in IT operations, developments and audits. The existence of several bodies that provide standards and certification for best practices within the U.S. and Europe provide evidence of the level of concern in the regions toward IT risks. This raises the issue of whether IT implementation in the other regions conforms to the standards established in the U.S. and Europe. Given the level of IT implementation by financial institutions

2 Japan and Hong Kong SAR are not members of SEACEN

within SEACEN countries, are best practices, the objectives of IT implementation by financial institutions, or is service provision the only thing that matters to them?

This research project is aimed at providing a comparative study on the IT implementation within SEACEN financial sectors, including its supervisory impacts, issues and challenges. The country papers are contributed by country researchers from the Ministry of Finance Brunei Darussalam; National Bank of Cambodia; Central Bank of the Republic of China (Taiwan); Bank Indonesia; Central Bank of Myanmar; The Bank of Mongolia; Nepal Rastra Bank; Central Bank of Sri Lanka; and State Bank of Vietnam. The Reserve Bank of Fiji, Bank Negara Malaysia, Bangko Sentral ng Philipinas, Monetary Authority of Singapore and Bank of Thailand contributed some data and information in their survey responses on IT implementation and IT supervisory framework in their respective countries. Two issues are worth mentioning here. First, since most of the central banks in the region are the authorities for the banking systems and not for non-bank financial institutions, the discussion on financial institutions focuses on banks. Second, in terms of financial engineering and financial product development, this region in general still follows the development established in the developed countries. The discussion therefore focuses on the second role: IT as the engine of operation (of financial institutions and markets). Indeed even in the developed countries, the risk of IT practices for the first role (as engine of financial development) has not been fully addressed, which has been a contributing factor to the ongoing global financial crises, in that risks associated with highly structured financial products have failed to be recognized due to lack of data and over-reliance on models and computer judgments.

SEACEN countries have different levels of IT implementation and IT supervisory framework. Three different levels of IT implementation can be found in these countries. They are: 1) Developed IT implementation and established IT supervisory framework; 2) Early stage of IT implementation with less-established IT supervisory framework; and 3) Less-developed IT implementation. In each level of implementation, countries face different issues and challenges. The consensus is that all countries – whenever IT implementation has become an important part of financial institution operation and management - consider IT supervision as an important part of the overall financial institution supervisory framework. However, since there is a cross-country heterogeneity of the IT implementation and IT supervisory framework, suggesting a minimum requirement for IT implementation in a financial institution and IT supervisory framework within SEACEN countries is a tough task. This research project is also a documentation on the development of IT implementation in financial institutions of SEACEN countries and the authorities' efforts to mitigate IT risks through IT supervisory frameworks.

This paper is organised as follows. Section 2 provides a summary of the above-mentioned international best practices within information technology (IT) and IT audit. This is deemed important to make an objective assessment of the IT practices by financial institutions and IT supervision in SEACEN countries. Section 3 discusses the cross-country comparison of IT implementation, the supervisory impact of the implementation and the supervisory framework installed in the financial institutions of SEACEN countries. Given the discussion in Section 3, Section 4 draws out some issues and challenges that SEACEN countries are facing related to IT implementation by financial institutions. Section 5 provides some suggestions to mitigate the risks and instigate the effort to establish a level playing field within SEACEN countries.

2. International Standards and Best Practices in Information Technology (IT) and IT Audit

This section provides a walk-through on the existing and most popular international guidance and best practices of information technology (IT) and IT audit. The focus is how useful the implementation of the standards or best practices contribute to the efforts to mitigate IT risk and to initiate an IT supervisory framework that conforms to internationally acceptable level. Conforming to the standards will make it easier for SEACEN countries to establish the credibility of their IT systems, and to expand their networks to international markets, thus facilitating more international financial transactions. For the purpose of introducing the standards and best practices and to refrain from getting into a detailed technical discussion, this Section provides a brief introduction on the contents of the standards and recommends interested readers to access the available resources for more detailed explanations.

The discussion on the standard practices becomes important to determine how well the SEACEN countries have managed the IT implementation in financial institutions. The Section is focused on the standards of ISO, COBIT, ITIL, FFIEC and the certification programmes of CISA, CISM and CISSP. The countries in the first group (countries with developed IT implementation with established IT Supervisory Framework) have already referred to some of the standards and best practices described in this Section.

2.1 ISO (International Organization for Standardization)

Although ISO is often considered an abbreviation for International Standards Organization, the use of the term ISO originally came from the Greek word '*isos*' which means equal. The International Organization for Standardization – based in Geneva, Switzerland – is the largest organisation that has been issuing international standards within business, government and society.

The family of ISO 27000[3] has been the most referred international standards for information security management system (ISMS). This is extremely important for financial institutions (FIs) implementing IT, both for their operations and R&D. FIs have to safeguard the integrity and security of client and customer information and financial data. The security issue has become one of the most important aspects in the overall IT implementation by financial institutions. It has also been the one that requires large investments. The security issue is always linked as the trade-off in providing easy access for clients (debtors) and customers (creditors/investors/depositors). The easier the access from outside of the FIs the higher the level of security measures that have to be implemented to guarantee the confidentiality and integrity of the data from the threat of unauthorised access.

ISO 27000 also addresses the complexity of providing standards for different types and sizes of organisations. ISO 27001, for example, provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System (ISMS). The 'process approach' of ISO 27001 also gives guidance to the design and implementation of an organisation's ISMS that is influenced by their needs and objectives, security requirements, the process employed and the size and structure of the organisation. ISO 27002 provides the standard code of practice for IT security that establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management within an organisation. The rest of ISO 27000 that has been issued provides standards for implementation of ISMS (ISO 27003), information security management measurements and metrics (ISO 27004), information security risk management (ISO 27005), and certification in information security (ISO 27006).

There are many online resources that are dedicated to providing information on ISO 27000, along with ISO which also provides online information in its web site. These resources include: http://www.27000.org, http://www.iso27001security.com, and http://standards.mobi/iso27000.htm. One critique for ISO standards is the fact that the documents are not available publically, and that companies have to pay for accessing the standards. However, by conforming to the ISO standards, companies receive reputational gain and competitive advantage. They will also have better opportunities to establish connections with international companies. In this case, FIs conforming to ISO standards will have a better chance to enlarge its captive market.

3 ISO 27000 or ISO 27k is the loose terms for ISO/IEC 27000. This is a family of international standards issued by the first joint technical committee (JTC1) between International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC).

2.2 COBIT (Control Objectives for Information and Related Technology)

COBIT is a set of standards for IT governance created by ISACA (Information System Audit and Control Association) and ITGI (Information Technology Governance Institute). First published in 1996, COBIT currently has been upgraded to version 4.1 (which was issued in May 2007). Unlike ISO 27000 that covers specifically information security matters, COBIT covers overall IT governance by providing a framework to ensure the IT system in an organisation is managed efficiently and effectively. The current COBIT focuses on five areas: strategic alignment, value delivery, resource management, risk management and performance measurement. COBIT is valuable for companies in determining exact decisions on IT investments, development and implementation. The guidance stipulated in COBIT is useful for companies that already consider information as a very important asset to support their overall objective.

Unlike ISO 27000, COBIT is available for free in ISACA's website http://www.isaca.org/cobit in different languages. Although not designed specifically for financial institutions, COBIT is a useful set of standards that can be implemented for financial institutions that value their IT resources highly.

2.3 ITIL (Information Technology Infrastructure Library)

ITIL is a registered trade mark of UK's Office of Government Commerce (OGC) which issues best practices for service management. Rather than describing the 'what', ITIL focuses on describing the process (the 'how'). This means that ITIL recommends processes instead of the elements of the system. The size, scope and depth of the IT system will depend on the business size and process. This means that ITIL is more flexible for implementation by companies or financial institutions of various sizes and different levels of business processes. ITIL was developed in coordination with ISO 20000 on IT Service Management Standard. In fact, the ISO standard actually refers to ITIL guidance. Currently, ITIL is the most popular standard for planning, provisioning and support of IT services.

The current ITIL (version 3) has been available since May 2007. This version takes the IT service management to another level by using the service life cycle approach, i.e. the processes involved in the evolution of service from creation to expiration. The standard includes five processes: 1) Service Strategy; 2) Service Design; 3) Service Transition; 4) Service Operation; and 5) Continual Service Improvement. These five standards are illustrated in Figure 1. More on ITIL is available in http://www.itil.org.

Figure 1

ITIL Service Lifecycle Approach

Source: ITIL Web Site http://www.itil.org

2.4 FFIEC (Federal Financial Institutions Examination Council) IT Examination Handbook

This Handbook is written as guidance for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), the Office of Thrift Supervision (OTS), and the State Liaison Committee (SLC). The SLC is comprised of representatives from the Conference of State Bank Supervisors (CSBS), the American Council of State Savings Supervisors (ACSSS), and the National Association of State Credit Union Supervisors (NASCUS). The objective of creating uniform principles, standards, and report forms in the federal examination is to have uniformity in the supervision of financial institutions. The complexity and increased integration of the U.S. financial system made this guidance extremely important for conducting consolidated supervision of financial institutions.

The FFIEC IT Examination Handbook provides a comprehensive set of information on the IT supervisory framework for financial institutions in the U.S. in a way that enables financial institutions to reach IT compliance. The Handbook covers a dozen of issues: 1) IT audit; 2) Business continuity planning; 3) Development and acquisition; 4) Electronic banking; 5) FedLine; 6) Information security; 7) Management; 8) Operations; 9) Outsourcing technology services; 10) Retail payment system; 11) Supervision of technology service providers; and 12) Wholesale payment systems. In terms of the context, this guidance is the most relevant for this research topic. The Federal Reserve Banks also refer to this guidance in the overall supervisory framework. Table 2.1 provides a brief description for each issue in the Handbook. This Handbook is available online at http://www.ffiec.gov/ffiecinfobase/html_pages/It_01.html.

Table 2.1

Federal Financial Institutions Examination Council 12 Issues in IT Examination Handbook

	Brief Description
IT Audit	The Audit Booklet provides guidance on the risk-based IT audit practices of financial institutions and technology service providers. This booklet builds on the agencies' existing audit guidance and emphasizes the responsibilities of all levels of management and the board of directors for establishing a sound audit program
Business Continuity Planning	The Business Continuity Planning Booklet provides guidance and examination procedures to assist examiners in evaluating financial institution and service provider risk management processes to ensure the availability of critical financial services. Sound business continuity plans allow financial institutions to respond to such adverse events as natural disasters, technology failures, human errors, and terrorism. Financial institutions must be able to restore information systems, operations, and customer services quickly and reliably after any adverse event. It is important that business operations be resilient and that customer service disruptions be minimal.
	The Development and Acquisition Booklet provides guidance on development, acquisition, and maintenance projects; project risks; and project management techniques. The booklet emphasizes the use of standardized policies, detailed plans, and well-structured project management techniques when directing project activities and controlling project risks. Effective development and acquisition should result in sound information systems that provide specific functionality, reliability, and strong security.

E-Banking	The E-Banking Booklet provides guidance on risks and risk management practices applicable to a financial institution's e-banking activities. E-banking has created new opportunities for delivering traditional products and services to customers, as well as the potential to offer new products and services. With these opportunities come new challenges, including 24-hour, seven-day-a-week availability; Internet connectivity; increased access to systems and customer information; greater reliance on new service providers; and evolving regulations. These challenges increase threats to the institution's reputation, confidentiality of information, system and data integrity, system availability, and regulatory compliance. E-banking activities require careful planning, coordinated strategies between IT and business units, integrated subject matter expertise, strong controls, and ongoing monitoring and testing. This booklet includes guidance and examination procedures to evaluate the quality of risk management related to these threats and activities in financial institutions and technology service providers.
FedLine	The FedLine® Booklet provides guidance on the appropriate control considerations for financial institutions using the Federal Reserve's FedLine® application. FedLine® provides financial institutions with access to the Federal Reserve's Fedwire services to receive and send payment messages. To protect their access to this system, institutions must ensure its security and availability. The booklet describes policies and procedures necessary to operate FedLine® in a safe and sound manner with detailed guidance on physical security, system configuration, and system parameter settings.
Information Security	The Information Security booklet provides guidance for examiners and financial institutions to use in identifying information security risks and evaluating the adequacy of controls and applicable risk management practices of financial institutions. The safety and soundness of the financial industry and the privacy of customer information depend on the security practices of banks, thrifts, credit unions and their service providers. The Information Security Booklet describes how an institution should protect the systems and facilities that process and maintain information. The booklet calls for financial institutions and technology service providers to maintain effective programs tailored to the complexity of their operations.
Management	The Management Booklet provides guidance on the risks and risk management practices applicable to financial institutions' information technology activities. Sound IT management is critical to the performance and success of a financial institution. An institution capable of aligning its IT activities to support its business strategies adds value to its organization and positions itself for sustained success. The board of directors and executive management should understand and take responsibility for IT management as a critical component of their overall strategic planning and corporate governance efforts.

Operations	The Operations Booklet provides guidance on the risks and risk management practices applicable to financial institutions' technology operations. Effective support and delivery from IT operations are vital to a financial institution's performance and success. The role that technology plays in supporting the business function has become increasingly complex. IT operations have become more dynamic and include distributed environments, integrated applications, telecommunication options, Internet connectivity, and an array of computer platforms. The booklet discusses tactical and strategic support and delivery risks, and the controls that should be in place to address those risks.
Outsourcing Technology Services	The Outsourcing Technology Services Booklet provides guidance on the risks and risk management practices applicable to financial institutions' outsourcing IT activities, including service provider selection, contract issues, and ongoing monitoring of the relationship. The booklet also includes guidance on the risks and risk management issues unique to foreign service providers. Outsourcing an activity does not relieve management and the board of directors of their responsibility to ensure a secure processing environment and the maintenance of data integrity. Thus, ongoing monitoring of the relationship is crucial to ensure the service provider follows the terms of the service level agreements, safeguards the confidentiality of information, and maintains operational stability.
Retail Payment System	The Retail Payment Systems Booklet provides guidance on the risks and risk management practices applicable to financial institutions' retail payment systems activities, including checks, card-based electronic payments, and other electronic payment media such as person-to-person, Electronic Benefits Transfer, and the Automated Clearinghouse. Financial institutions play an important role in retail payments, and will face many challenges as they implement new products and services. These challenges are a source of increased risk to institutions and require greater diligence to ensure the confidentiality of information, system and data integrity, system availability, and regulatory compliance. Retail payment system activities require careful planning for coordinated strategies between IT and business units, strong internal controls, and ongoing monitoring. The Retail Payment Systems Booklet includes guidance and examination procedures to evaluate the quality of risk management related to these risks and activities in financial institutions and technology service providers.
Supervision of Technology Service Providers	The Supervision of Technology Service Providers Booklet covers the supervision and examination of services performed for financial institutions by technology service providers. It outlines the agencies' risk-based supervision approach and the examination ratings used for technology service providers. The guidance stresses that an institution's management and board of directors have the ultimate responsibility for ensuring outsourced activities are conducted in a safe and sound manner and in compliance with applicable laws and regulations.

Wholesale Payment Systems	The Wholesale Payment Systems Booklet provides guidance on the risks and risk management practices applicable to financial institutions' wholesale payment systems activities, including interbank and intrabank payments, messaging, and securities settlement systems. Financial institutions play an important role in wholesale payments systems. However, they face increasing challenges to meet demands for resiliency and reliability, while continuing to develop and deploy innovative payment solutions to meet expanding global payment processing demands. Because of these challenges, institutions must exercise greater diligence to ensure that confidentiality of information, system and data integrity, system availability, and regulatory compliance are maintained. Wholesale payment system activities require careful planning and coordination between IT and business units, and their operation must include strong internal controls and ongoing monitoring. The Wholesale Payment Systems Booklet includes examination procedures to evaluate the quality of risk management related to these activities in financial institutions and technology service providers.

Note : The Information Technology Subcommittee will continue to oversee the maintenance of the original 12 booklets, and, when appropriate, will introduce additional booklets on new and emerging issues. This maintenance process ensures that the FFIEC IT Handbook remains current, establishes an equitable and flexible rotation and update process, provides ongoing tracking and oversight of needed revisions, and keeps the FFIEC website content current.

Source: FFIEC IT Examination Handbook Executive Summary (from http://www.ffiec.gov)

2.5 BCBS Risk Management Principles for Electronic Banking

Recognising the risk of the implementation of e-banking services, the Basel Committee on Banking Supervision (BCBS) introduced the risk management principles for electronic banking in 2001, updated in 2003. The 14 principles are established to help banking institutions expand their existing risk management framework to include the e-banking activities. Although e-banking risk is not considered a new risk, the existence of e-banking activities does increase, modify and complicate some of the traditional risks already inherent in the banking activities. The risk adds to the existing strategic, operational, legal and reputational risks.

The 14 risk management principles are grouped into three broad categories: 1) Board and management oversight (principles 1 to 3); 2) Security controls (principles 4 to 10); and 3) Legal and reputational risk management (principles 11 to 14). Although the principles are focused on e-banking activities, with some adjustments, they are suitable to address general issues related to IT implementation by banks. The BCBS Risk Management Principles are not developed to become "best practices" but rather to promote a sound and safe e-banking system. However,

for countries that are already oriented to the Basel II risk-based management, the 14 principals can be easily adopted to complete the overall risk management framework. Table 2.2 lists the 14 risk management principles for e-banking as recommended by the BCBS.

Table 2.2

Basel Committee on Banking Supervision's Risk Management Principles for Electronic Banking

Principle #	Principle Description
A. Board and Management Oversight (Principles 1 to 3)	
1	The Board of Directors and senior management should establish effective management oversight over the risks associated with e-banking activities, including the establishment of specific accountability, policies and controls to manage these risks.
2	The Board of Directors and senior management should review and approve the key aspects of the bank's security control process.
3	The Board of Directors and senior management should establish a comprehensive and ongoing due diligence and oversight process for managing the bank's outsourcing relationships and other third-party dependencies supporting e-banking.
B. Security Controls (Principles 4 to 10)	
4	Banks should take appropriate measures to authenticate the identity and authorization of customers with whom it conducts business over the internet.
5	Banks should use transaction authentication methods that promote non-repudiation and establish accountability for e-banking transaction.
6	Banks should ensure that appropriate measures are in place to promote adequate segregation of duties within e-banking systems, database and applications.
7	Banks should ensure that proper authorization controls and access privileges are in place for e-banking systems, databases and applications.
8	Banks should ensure that appropriate measures are in place to protect the data integrity of e-banking transactions, records and information.
9	Banks should ensure that clear audit trails exist for all e-banking transactions.
10	Banks should take appropriate measures to preserve the confidentiality of key e-banking information. Measures taken to preserve confidentiality should be commensurate with the sensitivity of the information being transmitted and/or stored in database.
C. Legal and Reputational Risk Management (Principles 11 to 14)	
11	Banks should ensure that adequate information is provided on their websites to allow potential customers to make an informed conclusion about the bank's identity and regulatory status of the bank prior to entering into e-banking transactions.
12	Banks should take appropriate measures to ensure adherence to customer privacy requirements applicable to the jurisdiction to which the bank is providing e-banking products and services.

13	Banks should have effective capacity, business continuity and contingency planning processes to help ensure the availability of e-banking systems and services.
14	Banks should develop appropriate incident response plans to manage, contain and minimize problems arising from unexpected events, including internal and external attacks, that may hamper the provision of e-banking systems and services.

Source: Basel Committee on Banking Supervision, Risk Management Principles for Electronic Banking, July 2003 (BCBS 2003a)

In addition to the 14 risk management principles for e-banking, BCBS also published a paper titled "Management and Supervision of Cross-Border Electronic Banking Activities" in 2003. Cross-border e-banking is defined as provision of on-line banking products or services remotely from one country to residents in another country (BCBS 2003a). The paper highlights the recognition of the risk inherent in cross-border e-banking activities and calls to attention the necessity for the home country to supervise cross-border e-banking activities and pursue international cooperation with regard to supervision of such activities. The documents mentioned in this sub-section are available at http://www.bis.org.

2.6 Certification Programmes: CISSP, CISA and CISM

As the business world becomes more dependent on IT systems, the successful design and implementation of the IT systems become crucial. The IT society has developed many certification programmes for varying layers of IT systems to ensure this. IT security has become the most important layer of IT implementation considering the nature of the information handled in the financial institutions. For IT security, CISSP (Certified Information Systems Security Professional), CISM (Certified Information Security Manager), and CISA (Certified Information System Auditor) are three of the most popular certification programmes.

The CISSP programme is designed to recognise the standard level of knowledge for information system security that is in essence covered by the 10 information security domains or 10 common body of knowledge (CBK). These are: 1) Access control; 2) Application security; 3) Business continuity and disaster recovery planning; 4) Cryptography; 5) Information security and risk management; 6) Legal, regulations, compliance and investigations; 7) Operations security; 8) Physical (environmental) security; 9) Security architecture and design; and 10) Telecommunications and network security. All these 10 domains are relevant to the IT implementation by financial institutions. To become a CISSP, one needs to pass the CISSP examination, and also to fulfill minimum requirements in terms of professional experience, having a crime free history and related background as well as be in good standing within the information security industry. CISSP is governed by the International Information System Security Certification Consortium (or commonly known as (ISC^2)). More information is available at http://www.isc2.org.

The ISACA (Information System Audit and Control Association) – the organisation that issues COBIT - also conducts two different certification programmes related to IT security. They are CISM and CISA. CISM (Certified Information Security Manager) focuses on information risk management and is designed for individuals who manage, design, oversee and assess an enterprise's information security system. To earn the CISM, an individual must pass a written examination and have at least five years experience in information security and three years of information security management work experience in particular fields. The CISA (Certified Information System Auditor) is designed for those focusing on the tasks of controlling, monitoring and assessing an organisation's information technology and business systems. In addition to passing the examination, requirements to earn the CISA can be substituted between academic semester credit hours or full-time university instructor years and professional experience, all in fields related to information systems auditing, control or security experience. More information on CISM and CISA is available at http://www.isaca.org.

3. Cross-Country Comparison

Amongst the 16 SEACEN member central banks, 9 participated in this research project, namely Ministry of Finance, Brunei Darussalam; National Bank of Cambodia; Central Bank of the Republic of China (Taiwan); Bank Indonesia; Bank of Mongolia; Central Bank of Myanmar; Nepal Rastra Bank; Central Bank of Sri Lanka; and State Bank of Vietnam. The Reserve Bank of Fiji, Bank Negara Malaysia, Bangko Sentral ng Pilipinas, Monetary Authority of Singapore and Bank of Thailand contributed by responding to the survey designed especially for this research project. The cross-country comparison is based on the data and information found in the country papers and survey responses.

The participating country researchers agreed to focus on banking financial institutions for this project. This is hardly surprising since banks are still dominating the regional financial markets. Most central banks in the region are the authorities for the banking sector only while other institutions in the financial system fall under the supervisory purview of the Ministries of Finance.[4] However, although this will not be in the cross-country comparison, depending on the availability of data, some country papers will include some information about the non-bank financial institutions (NBFI).

Because of the heterogeneity of IT implementation and IT supervisory framework in the region, the survey was designed to discover whether there is a specific aspect of IT implementation by banks or particular IT supervisory framework being implemented in a country. The information on the quantity and

4 In the case of Brunei Darussalam which does not have a central bank, the Ministry of Finance is the single authority of the entire financial system. In the case of the Central Bank of the Republic of China (Taiwan), the central bank is not the supervisory authority of the banking system. The Reserve of Bank of Fiji is the authority for banking, insurance, foreign exchange and superannuation industries.

the quality of the implementation is left to the country researchers to discuss in the country papers.

3.1 IT Implementation

The survey requested for information on the state of IT infrastructure, IT implementation in general, and IT implementation by banks. The first significant finding was presented at the early stage of the research project. This is related to the level of IT implementation across the SEACEN member countries. In terms of communication infrastructure, various networks (phone, satellite, fiber optic) have been developed in all countries. Although they are not very widespread in some countries, the use of cellular phones and the internet are common in the region. The widespread use of the internet and cellular phones is a separate issue in itself. For countries with many islands like Fiji, Indonesia and the Philippines, establishing standard communication infrastructures for the entire region of the country is a challenge in itself. With the exception of Brunei Darussalam, a national payment system exists in all countries in the region. However, Cambodia, Myanmar and Nepal still rely on a manual payment system, using tickets representing banking transactions. From the countries in observation, the ASEAN big five (Indonesia, Malaysia, the Philippines, Singapore and Thailand) and the Republic of China (Taiwan) – the latter from here onward will be mentioned as Taiwan – are the countries with more advanced infrastructures. These countries are equipped with national payment systems – including the real time gross settlement (RTGS) – and national securities settlement systems. The level of IT implementation in the SEACEN member countries is then subject to the availability of technology infrastructure, the support of the payment system, and demand-driven financial service development. The latter also depends on how widespread the use of high technology gadgets is in a particular country. Singapore – already regarded as one of the most IT literate society in the region – certainly has a high level of IT implementation, comparable to international standards, while the Central Bank of Myanmar still disallows the usage of IT in their banking system after many cases of illegal financial operations by general service enterprises in 2003, and has since then not permitted banks to implement IT to support their operations up to the conclusion of this project. Table 3.1 provides the survey result on the IT infrastructure of the countries under observation.

The survey also reveals the state of e-banking implementation in SEACEN member countries. With the exception of Myanmar, all survey respondents participating in the research indicated that some to all of the e-banking products in questions exist in their countries. The products in questions include credit card, debit card, ATM, Electronic Fund Transfer (EFT), EFT at Point of Sale, Remittance Service, Phone Banking, Mobile/SMS Banking, Internet Banking, and Pre-paid card with the Credit card, Debit card, ATM and EFT being the most popular products. In the case of ATM services, banks in Brunei and Cambodia still maintain

provision of individual bank ATM services. Internet banking is surprisingly more available than phone banking and mobile/SMS banking. Cambodia, for example, has internet banking service, but does not have mobile/SMS and phone banking services. In Myanmar, the absence of an EFT system in the banking system is covered by remittance services from a domestic company. Myanmar also relies on the SWIFT (Society Worldwide Inter-bank Financial Telecommunication) system provided by the Central Bank of Myanmar and state-owned banks to carry out international payment and settlement transactions. Stating not to have widespread use of mobile phones outside the two main islands, Fiji does not have mobile/SMS banking service. However, this could also be the result of the convenience of internet banking that already provides the means for doing remote transactions. Although phone, mobile/SMS or internet banking are implemented, interbank transaction services are not provided in Brunei, Cambodia, Mongolia, Sri Lanka and Vietnam. Malaysia also does not provide the interbank transaction feature in its mobile/SMS banking. All in all, the survey results show that SEACEN countries do not shy away from e-banking products. Given the population of approximately 575 million people[5], the SEACEN region is a potential market for banks to implement e-banking to increase their fee-based income. Table 3.2 provides the survey results of the e-banking products implemented in SEACEN countries.

5 The population number refers to the combined populations in the ASEAN countries only.

Table 3.1
IT Infrastructure Survey

No.	Item	BRU	CAM	FIJ	INA	MAL	MON	MYA	NEP	PHI	SIN	SRI	TAI	THA	VIE
1	Communication Network	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
	Cable (Phone line)	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
	Satellite	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
	Fiber Optic	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
2	Use of Cellular Phone	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
	Is it relatively wide spread?	Y	Y		Y	Y	Y			Y	Y	Y	Y	Y	Y
3	Use of Internet	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
	Is it relatively wide spread?	Y				Y	Y			Y	Y	Y	Y	Y	Y
4	National Payment System		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
5	Operated by government agency / central bank		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
6	Operated by an independent or private company	Y		Y	Y	Y				Y	Y		Y	Y	
7	Automated/Computerized Payment System	Y		Y	Y	Y	Y			Y	Y	Y	Y	Y	Y
8	RTGS			Y	Y	Y				Y	Y	Y	Y	Y	Y
9	National Securities Settlement System			Y	Y	Y	Y			Y	Y	Y	Y	Y	
	Operated by government agency / central bank			Y	Y		Y			Y	Y	Y	Y	Y	Y
	Automated/Computerized Settlement System				Y	Y				Y		Y	Y	Y	Y

Notes: Y refers to the reply "Yes" in the question: "Are the following IT infrastructure installed in the country?"

If a country reply "Yes" to both No. 5 and 6, it means the national payment system is run by both government agency / central bank and private companies.

BRU: Brunei Darussalam, CAM: Cambodia, FIJ: Fiji, INA: Indonesia, MAL: Malaysia, MON: Mongolia, MYA: Myanmar, NEP: Nepal, PHI: the Philippines, SIN: Singapore, SRI: Sri Lanka, TAI: Republic of China (Taiwan), THA: Thailand, VIE: Vietnam.

Table 3.2
E-Banking Products

No.	Item	BRU	CAM	FIJ	INA	MAL	MON	MYA	NEP	PHI	SIN	SRI	TAI	THA	
1	Credit Card	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	
	National (only used in the country)	Y	Y		Y	Y	Y		Y	Y	Y	Y	Y	Y	
	International	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	
2	Debit Card	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	
	National (only used in the country)	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	
	International			Y	Y		Y		Y	Y	Y	Y	Y	Y	
3	ATM	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	
	Individual bank	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	
	Nationally-Shared ATM			Y	Y	Y			Y	Y	Y		Y	Y	
	Internationally-Shared ATM			Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	
4	Electronic Fund Transfer (EFT)	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	
5	EFT at Point of Sale	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	
	National (only within the country)	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	
	International	Y		Y	Y		Y		Y	Y	Y	Y	Y	Y	
6	Remittance Service	Y		Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	
	Domestic companies	Y		Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	
	International companies	Y		Y	Y	Y	Y		Y	Y	Y		Y	Y	
7	Phone Banking	Y		Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	
	Informational	Y		Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	
	Transactional intra bank	Y		Y	Y	Y			Y	Y	Y	Y	Y	Y	
	Transactional inter bank				Y	Y				Y	Y		Y	Y	
8	Mobile/SMS Banking	Y			Y	Y	Y		Y	Y	Y	Y	Y	Y	
	Informational	Y			Y	Y	Y		Y	Y	Y	Y	Y	Y	
	Transactional intra bank	Y			Y	Y				Y	Y	Y	Y	Y	
	Transactional inter bank				Y					Y	Y		Y	Y	
9	Internet Banking	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	
	Informational	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	
	Transactional intra bank	Y	Y	Y	Y	Y	Y		Y	Y	Y		Y	Y	
	Transactional inter bank				Y	Y				Y	Y	Y	Y	Y	
10	Pre-paid card	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	

Notes: Y refers to the reply "Yes" to the question: "Are the following IT-related products implemented in the country?".

BRU: Brunei Darussalam, CAM: Cambodia, FIJ: Fiji, INA: Indonesia, MAL: Malaysia, MON: Mongolia, MYA: Myanmar, NEP: Nepal, PHI: the Philippines, SIN: Singapore, SRI: Sri Lanka, TAI: Republic of China (Taiwan), THA: Thailand, VIE: Vietnam.

The Republic of China (Taiwan) country paper in this research project provides an interesting way of categorising the IT implementation by banks. They are: Category A – Banking Business Applications; Category B – E-banking systems; and Category C – Management Information System. Category B is self explanatory as it was just discussed in the previous paragraph. Category A refers to computerised system for the banking business, which includes all the applications for deposit, loan, foreign exchange, treasury, trustee, credit cards, remittance, ATM, etc. However, the extent of this category is only for what affects the internal process in the bank. IT applications become part of category B when they are built to allow access through electronic channels by outside parties. When the applications are built to support the decision making process within the bank management, they fall into category C. Many banks implement IT only for the purpose of automation and provision of better services. Modern banks would manage the information that they have in hand to aid them in the research and development of products and services as well as in making informed decisions for the benefit of the bank. This is why decisions on IT implementation will generate a certain IT risk as part of the strategic risk. For this reason, the standards of IT implementation require IT decisions to be made by the top management.

In addition to the e-banking applications, with the exception of Cambodia and Myanmar, SEACEN member countries implement other applications to support banking business. Brunei, Fiji, Indonesia, Malaysia, Nepal, the Philippines, Singapore, Sri Lanka, Taiwan, and Thailand implement all the applications for core banking (general ledger, deposit, loan, and consumer information), treasury, remittance, trade finance, and corporate online service. Mongolia does not have corporate online services, while Vietnam only has the computerised core banking and remittance processes. This shows that there is a large potential for managing information to support the decision making process. If the information generated by the IT implementation in banks is used for the development of financial products and services, then this is where IT plays the first role discussed in the first Section. Table 3.3 provides the survey results on the banking application excluding e-banking.

Table 3.3
Banking Applications Excluding E-Banking

No.	Item	BRU	CAM	FIJ	INA	MAL	MON	MYA	NEP	PHI	SIN	SRI	TAI	THA	VIE
1	Core Banking: General Ledger, Third Party Fund, Loan, and Consumer Information File	Y		Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y
2	Treasury	Y		Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	
3	Remittance	Y		Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y
4	Trade Finance	Y		Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	
5	Corporate Online Service	Y		Y	Y	Y			Y	Y	Y	Y	Y	Y	

Notes: Y refers to the reply "Yes" to the question: "Regarding IT-related applications in addition to IT-related products, are the following applications implemented with IT?" Cambodia (CAM) and Myanmar (MYA) reply "No" to all questions

BRU: Brunei Darussalam, CAM: Cambodia, FIJ: Fiji, INA: Indonesia, MAL: Malaysia, MON: Mongolia, MYA: Myanmar, NEP: Nepal, PHI: the Philippines, SIN: Singapore, SRI: Sri Lanka, TAI: Republic of China (Taiwan), THA: Thailand, VIE: Vietnam.

3.2 Supervisory Impacts of IT Implementation

With the level of IT implementation in the region, especially with the relatively high exposure to the e-banking products, one then can question the impact of the implementation on the banks. The IT implementation should have benefits that exceed the costs to cover for IT problems when they happen (IT risks). Under risk-based management by banks, IT risks should be incorporated in the overall risk management. While the existing risk management frameworks are still applicable, the risks posed by e-banking activities and the growing reliance of the banks on IT systems in conducting their everyday business have to be recognised.

BCBS categorises IT risks as part of the strategic, operational and legal risks. These are the risks already identified within the risk-based management framework. However, this has not stopped Singapore from defining IT risk as a separate risk from the other risks already identified in the existing risk-based management framework. Nevertheless, the survey results show that most SEACEN member countries already recognise IT risks as part of operation, liquidity, credit, strategic, reputation, legal and compliance risks. Operation risk is the risk associated with the possibility of failures, errors or any forms of actions that may halt or delay bank services. The IT failures can have direct effect on the reliability of the banking operations. Liquidity risk is the risk associated with not being able to cover the liabilities when they fall due. The use of IT system enables transactions to be executed very quickly and it can drain the bank's liquidity in a matter of seconds. Credit risk is associated with the possibility that the counterparty cannot fulfill its obligation when it falls due. The use of IT system for gaining new clients (debtors) sometimes disregards the assessment on the creditworthiness of the client. Strategic risk is associated with the possibility of the top management making the wrong business decision for the bank. The wrong decision on the IT design and implementation can cost the bank a large investment and reduce their competitiveness with other banks. Reputation risk involves the possibility that customers (depositors) and clients (debtors) may be reluctant to do transactions with a bank because they hear some bad news about the bank. Improper IT implementation can spread as bad news and cost a bank its reputation. Legal risk is associated with the possibility of the bank having to deal with legal procedures with its counterparty. IT implementation without proper agreement between bank and clients/customers can increase the bank's legal risk. Compliance risk is associated with the bank having to deal with the banking authority because it does not comply to the banking regulations. The mechanism of electronic transaction sometimes only puts emphasis on the ease and speed of the process, but disregards the possibility that it may bypass some regulations imposed by the authority.

Stating not to have nationally-shared ATMs and transactional inter-bank features in their phone banking, mobile/SMS banking and internet banking, Malaysia and Sri Lanka do not think that IT poses additional risks in terms of

liquidity and creditworthiness. With its current level of IT implementation, Vietnam also does not consider IT risk as inherent in the reputation, legal, and compliance risks of Vietnamese banks. Table 3.4 provides the overall results of the survey on IT risks.

3.3 IT Supervisory Framework

Recognising that IT risks is inherent in the IT implementation by banks, central banks are now embarking on establishing IT supervisory frameworks. It is not surprising to find that the SEACEN member countries with a higher level of IT implementation by banks are also the countries with the more established IT supervisory framework. Fiji, Indonesia, Malaysia, Mongolia, the Philippines, Singapore, Sri Lanka, the Republic of China (Taiwan) and Thailand have formal frameworks installed. However, only Indonesia, the Philippines, Singapore, Sri Lanka and the Republic of China (Taiwan) have formalised their frameworks by regulations. The other countries have the IT supervisory frameworks embedded in their guidelines for overall bank supervision practices. Although it is not a formal framework, Cambodia conducts IT supervision during the regular supervision and requires banks to have a minimum requirement on IT implementation. Although without a formal IT supervisory framework, the State Bank of Vietnam conducts IT audits on certain items of IT systems in banks.

The ASEAN big five and Taiwan designed specific IT supervisory frameworks using risk-based management approach. Thailand makes reference to the guidelines from the FFIEC while Malaysia refers to the risk-based supervisory framework (RBSF) adopted by Canadian Office of the Superintendent of Financial Institutions, FFIEC and COBIT. The Philippines makes reference to FFIEC and COBIT while Indonesia combines references from FFIEC, COBIT, ISO on IT Security and Management, ITIL, as well as studies of the frameworks in Hong Kong, Malaysia and Singapore. The rest of the countries with formal IT supervisory framework incorporate their IT supervision in their regular supervision practices. With the exception of Fiji, it is also not surprising to find that countries with established IT supervisory framework also already have higher level legal frameworks that address IT practices in general[6]. The growing references on the best practices in IT management and security as well as the experiences of the countries that already have established IT supervisory frameworks should be useful for countries planning to set up their IT supervisory framework. Funding is also available to finance the development of IT supervisory framework. For example, Bank of Mongolia developed the IT supervisory framework with funding from JICA (Japan International Cooperation Agency). The survey results on the current state of IT supervisory frameworks in SEACEN member countries are shown in Table 3.5.

---

6 Higher level legal frameworks regarding IT practices generally include cyber law, and laws on e-commerce, m-commerce, and digital signature.

Table 3.4
IT Risks

No.	Item	BRU	CAM	FIJ	INA	MAL	MON	MYA	NEP	PHI	SIN	SRI	TAI	THA	VIE
1	Operation Risk	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y
2	Liquidity Risk	Y	Y	Y	Y		Y		Y	Y	Y		Y	Y	Y
3	Credit Risk	Y	Y	Y	Y		Y		Y	Y	Y		Y	Y	Y
4	Strategic Risk	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y
5	Reputation Risk	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	
6	Legal Risk	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	
7	Compliance Risk	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	

Notes: Y refers to the reply "Yes" to the question: "As the impact of the level of IT implementation in the country, what are the risks that need to be addressed and controlled in the financial system?" Myanmar (MYA) does not have IT implementation in the financial institutions, therefore is not exposed to any IT Risks. Singapore (SIN) actually has IT Risk as a separate risk, and not inherent in the other risks.

BRU: Brunei Darussalam, CAM: Cambodia, FIJ: Fiji, INA: Indonesia, MAL: Malaysia, MON: Mongolia, MYA: Myanmar, NEP: Nepal, PHI: the Philippines, SIN: Singapore, SRI: Sri Lanka, TAI: Republic of China (Taiwan), THA: Thailand, VIE: Vietnam.

Table 3.5
IT Supervisory Framework

No.	Item	BRU	CAM	FIJ	INA	MAL	MON	MYA	NEP	PHI	SIN	SRI	TAI	THA	VIE
1	Is IT Implementation reported regularly?		Y	Y	Y	Y				Y	Y	Y			Y
2	Is IT audit conducted?	Y	Y	Y	Y	Y	Y			Y	Y	Y	Y	Y	Y
	By bank/IT supervisors from supervisory authority			Y	Y	Y				Y	Y	Y	Y	Y	Y
	Off-site				Y	Y					Y			Y	Y
	On-site			Y	Y	Y	Y			Y	Y	Y	Y	Y	
	By internal or external (third party) auditors (on-site)	Y	Y	Y	Y	Y				Y	Y	Y	Y	Y	
	Special IT audit/examination outside regular examination (on-site)		Y		Y	Y				Y			Y	Y	
3	Does the formal framework exist?			Y	Y	Y	Y			Y	Y	Y	Y	Y	
4	If yes, is it stipulated in a regulation?				Y					Y	Y	Y	Y		
5	Is there minimum requirement in IT Implementation?		Y	Y	Y	Y				Y	Y		Y	Y	Y
	Are the following items implemented:														
	Active supervision by Top Management (IT Steering Committee)		Y	Y	Y	Y	Y			Y	Y	Y	Y	Y	
	IT Policy and Standard Operating Procedure		Y	Y	Y	Y	Y			Y	Y	Y	Y	Y	
	IT risk is included in the risk-based management		Y	Y	Y	Y	Y			Y	Y	Y	Y	Y	
	System development life cycle		Y	Y	Y	Y	Y			Y	Y	Y	Y	Y	Y
	All layers of IT system		Y	Y	Y	Y	Y			Y	Y	Y	Y	Y	Y
	Internal control system for IT Implementation		Y	Y	Y	Y	Y			Y	Y	Y	Y	Y	
	Business Continuity Plan and Disaster Recovery Plan		Y	Y	Y	Y	Y			Y	Y	Y	Y	Y	Y
	Periodical IT audit (internal/external)		Y	Y	Y	Y	Y			Y	Y	Y	Y	Y	
6	Because it involves supervision procedure, is IT outsourcing especially regulated?		Y		Y	Y	Y			Y	Y	Y	Y	Y	Y
7	Because it involves consumer protection, is E-banking products especially regulated?		Y		Y	Y	Y			Y	Y	Y	Y	Y	Y
8	Are any IT-related laws (cyber law, e-commerce, m-commerce, digital signature) installed?	Y			Y	Y				Y	Y	Y	Y	Y	Y

Notes: Y refers to the reply "Yes" to each question in the column Item. Nepal (NEP) and Myanmar (MYA) reply "No" to all questions.

BRU: Brunei Darussalam, CAM: Cambodia, FIJ: Fiji, INA: Indonesia, MAL: Malaysia, MON: Mongolia, MYA: Myanmar, NEP: Nepal, PHI: the Philippines, SIN: Singapore, SRI: Sri Lanka, TAI: Republic of China (Taiwan), THA: Thailand, VIE: Vietnam.

IT audit refers to an on-site examination of the IT system by bank supervisors. In this case, countries with formal IT supervisory framework do not necessarily conduct regular IT audits. Fiji and Vietnam only conduct IT audit whenever it is necessary. When it is conducted regularly, the items of IT systems examined include: 1) organisation and management; 2) system development process; 3) operation; 4) software and application, including e-banking; 5) security; 6) business continuity planning (BCP) and disaster recovery planning (DRP); 7) communication network; 8) outsourcing process; and 9) internal auditing. Although Mongolia has not started IT audits yet, the Bank of Mongolia has all the items listed included in the IT audit within the IT supervisory framework that will take effect in the banking system starting 2010. The result of the survey on IT audit is presented in Table 3.6.

3.4 Facts and Findings

The state of IT implementation and IT supervisory framework in the SEACEN member countries illustrate the heterogeneity of IT practices within the region. This poses difficulties in the effort to bring the region into a level playing field in terms of IT implementation by financial institutions. In general, there are three different levels of IT implementation found in the region: 1) Developed IT implementation with established IT supervisory framework; 2) Early stage of IT implementation with less-established IT supervisory framework; and 3) Less-developed IT implementation. However, this should not discourage the countries that fall into the second or third groups as there are many opportunities of spillover of knowledge and expertise within the region to improve the financial institutions' IT practices. The supervisory frameworks of some SEACEN member countries are listed in Table 3.7.

The prevailing IT supervisory frameworks in the region can also be grouped into two different models. In the first model, the IT supervisory framework is addressed as a separate issue from the supervisory framework for banks. In the second model, IT supervision becomes a part of the overall banking supervision practices. The first model is implemented by countries with banks that use relatively more sophisticated IT systems. This model usually requires the supervisory authority to pay special attention to the conduct of IT audits - up to the level requiring IT specialists for the IT audits. The Philippines, for example, created the Core Information Technology Specialist Group (CITSG) composed of Certified Information Systems Auditors (CISA) that focuses on IT supervision only. Bank Indonesia also employs IT specialists to do the IT audits.

Table 3.6
IT Audit

No.	Item	BRU	CAM	FIJ	INA	MAL	MON	MYA	NEP	PHI	SIN	SRI	TAI	THA	VIE
1	Is it conducted regularly?		Y		Y	Y				Y	Y	Y	Y	Y	
2	If not regularly, is it conducted case by case?			Y											Y
3	If regularly, objects of audit:														
	Organization and Management		Y	Y	Y	Y	Y			Y	Y	Y	Y	Y	
	System development process		Y	Y	Y	Y	Y			Y	Y	Y	Y	Y	
	Operation		Y	Y	Y	Y	Y			Y	Y	Y	Y	Y	
	Software and Application, including E-Banking		Y	Y	Y	Y	Y			Y	Y	Y	Y	Y	
	Security (authentication, authorization and protection– including audit trails, encryption)		Y	Y	Y	Y	Y			Y	Y	Y	Y	Y	
	BCP/DRP		Y	Y	Y	Y	Y			Y	Y	Y	Y	Y	
	Communication Network		Y	Y	Y	Y	Y			Y	Y	Y	Y	Y	
	Outsourcing process		Y	Y	Y	Y	Y			Y	Y	Y	Y	Y	
	Internal Auditing		Y	Y	Y	Y	Y			Y	Y	Y	Y	Y	

Notes: Y refers to the reply "Yes" to each question in the column Item. Mongolia (MON) replies no to both of first two questions, but plans to do IT audits on all of the objects listed in question 3. Fiji (FIJ) does not have regular IT audit, however when IT audit is conducted, all of the objects listed in question 3 are included. Brunei (BRU), MYA (Myanmar), Nepal (NEP) reply "No" to all questions.

BRU: Brunei Darussalam, CAM: Cambodia, FIJ: Fiji, INA: Indonesia, MAL: Malaysia, MON: Mongolia, MYA: Myanmar, NEP: Nepal, PHI: the Philippines, SIN: Singapore, SRI: Sri Lanka, TAI: Republic of China (Taiwan), THA: Thailand, VIE: Vietnam.

Table 3.7

Formal IT Supervisory Frameworks in SEACEN

Supervisory Authority	Supervisory Framework
Reserve Bank of Fiji	No specific framework, IT examination is incorporated in the regular supervisory framework
Bank Indonesia	Bank Indonesia Regulation No. 9/15/PBI/2007 regarding Risk Management in the Use of IT by Commercial Banks
Bank Negara Malaysia	Guidelines on Management of IT Environment (GPIS 1)
Bank of Mongolia	IT Inspection guideline, manual, handbook and standards.
Banko Sentral ng Philipinas	Technology Risk Management, Consumer Prostection on Electronic Banking, Guidelines on the Provision of Electronic Banking Products, Outsourcing Service, and Business Continuity Planning.
Monetary Authority of Singapore	Electronic Common Risk Assessment for Technology (eCRAFT)
Central Bank of Sri Lanka	IT Supervisory Framework of Central Bank of Sri Lanka
Financial Supervisory Commission of the Executive Yuan (Republic of China - Taiwan)	Rules governing Information Security Management of Executive Yuan and Organizations under the Yuan, Rules for Internal Audit and Internal Control System, Information System Security Standards for Financial Institutions, Risk Management Principles for Electronic Banking, and Guidelines for Security Measures of Financial Institutions for Electronic Banking Service.
Bank of Thailand	IT Risk-based Supervision (no specific name mentioned for the framework)

Source : Country papers and survey responses to this research project.

The IT risk-based supervision is also considered the best approach by the countries with the more established IT supervisory framework. This approach is already compatible with the overall risk-based supervision suggested by Basel II Framework. However, this risk-based approach is sometimes considered being too reliant on the financial institutions assessing their own IT risks. In order to bridge this gap, IT supervisors have to conduct IT risk profiling first. For example, Indonesia requires banks to submit reports on their IT implementation and acquire Bank Indonesia's approval before implementing IT-related or e-banking products so that potential IT risk can be captured early. Using the risk-focused approach, Singapore's eCRAFT enables supervisors of the Monetary Authority of Singapore to calibrate the intensity and frequency of IT supervision for certain financial institutions. Nevertheless, the risk-based approach is not the only approach available for IT supervisory framework. Referring to the best practices discussed in Section 2, countries can also refer to the minimum requirement for the processes

that need to be done in an IT system environment. This will be more flexible for financial institutions that may only implement a simple IT system that will not require highly skilled IT supervisors.

It is important for the countries planning to establish and improve their IT supervisory frameworks to balance between efficiency and efficacy in the implementation of the frameworks. While IT implementation should not be discouraged, the IT risks need to be controlled. The intensity of IT supervision should also be determined by the level of IT implementation in the financial institutions. The complexity of the IT supervisory framework should also be determined by the level of IT implementation and IT risks in the financial industry.

4. Issues and Challenges

The state of IT implementation and IT supervisory framework in SEACEN member countries raises issues and challenges that need to be addressed by the efforts taken by the individual countries as well as by concerted efforts from all the SEACEN member countries. IT risk is an integrated part of the overall risks that a financial institution runs in conducting its business. However, the heterogeneity in the IT implementation and the state of IT supervisory frameworks of SEACEN member countries present different sets of issues to the three different groups of countries identified earlier. This research study identifies some common issues and challenges faced in the region, although the intensity levels can be different across countries. The levels of IT implementation in this section refer to the three different levels of IT implementation found in the region described in the beginning of section 3.4.

4.1 Issues

4.1.1 The Lack of IT Awareness

IT awareness is related to the awareness by the banking society (banks and bank customers) and bank supervisors. In the case of countries in level 1 of IT implementation, this issue is related to the awareness of bank customers about the mechanism of IT-supported products, and the risks that they are facing when they do not put sufficient emphasis on the IT security aspect of the products and ensure the privacy and integrity of their own financial information. Countries in the level 2 IT implementation are more concerned about the awareness of banks on the standards of their IT practices and the awareness of the bank supervisors about the inherent risk in the IT implementation by banks. The lack of IT awareness leads to the negligence of IT risks that can potentially cause IT failure that may halt operations resulting in repair, recovery and opportunity cost.

4.1.2 Higher Level Legal Base

Efforts to increase the level of a legal framework on IT practices are still needed. This is a requirement for all countries for the effective enforcement in implementing good IT governance as well as preventing irresponsible behaviour related to IT implementation. A stronger legal infrastructure provides a stronger foundation in enforcing the IT supervisory framework and promotes IT awareness in society. For countries that have not established their IT supervisory frameworks, the law on IT practices in the country can become the foundation for their IT supervisory frameworks.

4.1.3 The Development of IT Infrastructure

The development of IT infrastructure is also an issue that needs to be addressed continuously. For countries with level 1 IT implementation, the development of IT infrastructure will be focused on the provision of a more efficient and cheaper communication service and payment system without sacrificing the integrity and security of the systems. For countries in level 2 and 3, the development will be focused on the provision of communication technology that can support the inter-bank network and connection to bank customers. This includes having an effective IT-supported national payment system and RTGS.

4.1.4 The Heterogeneity of IT Implementation

The heterogeneity of the IT implementation within one country as well as across countries in the region raises the issue of compatibility among IT systems of SEACEN financial institutions. This also raises an issue of having a minimum standard for IT implementation in the region. The different levels of IT implementation also requires different intensities of IT supervision.

4.1.5 Improvement of IT Security

IT security is always an important aspect in IT implementation by financial institutions. Countries in group 2 and 3 still have some ways to go to before the quality of their IT security meets best practices. Countries in group 1 are focusing on the more sophisticated methods for IT security since the financial institutions in these countries are becoming more dependent on IT systems.

4.1.6 Enforcement of IT Good Governance

Enforcement of IT risk management in the financial institutions is another issue faced by the countries in review. Countries in group 1 are focusing on enforcement of their IT supervisory frameworks, while countries in group

2 are incorporating IT examination in their bank supervision practices and improving their IT supervisory framework. Enforcing IT risk management will help increase IT good governance by financial institutions.

4.2 Challenges

1. Bringing IT implementation in SEACEN financial institutions to a level playing field.

   Given the state of IT implementation in SEACEN member countries, bringing the IT implementation by SEACEN financial institutions to a level playing field becomes a challenge. This challenge becomes even more urgent with the plan to initiate the ASEAN Economic Community in 2015. The strong relationship amongst the SEACEN member countries makes it possible to promote IT awareness in the region and spillover of knowledge of IT implementation to accelerate the process.

2. Establishing effective prudential regulations in IT implementation

   The competition amongst financial institutions in implementing IT can create a kind of "euphoria" in IT development with disregard to issues of security and integrity which can lead to reckless IT practices. Central banks, as the banking authorities, are challenged to implement effective prudential regulations to ensure IT risks can be controlled. In this way, the benefits of IT implementation can be gained without sacrificing the integrity of the financial institutions.

3. Improving IT risk management

   The challenge to improve IT risk management in the region with or without formal IT supervisory frameworks is always there in any country. Central banks should also take advantage of the availability of standards and best practices for IT management and security in designing and improving their IT supervisory framework. Learning from the strengths and weaknesses of the frameworks implemented in other countries is also essential. This can be encouraged in the SEACEN region, since there are already countries with established IT supervisory frameworks and thereby able to share their experiences in designing their frameworks.

4. Keeping up with the global financial market

   The increasing integration of the global financial market has made cross border e-banking products additional services offered by banks with sophisticated IT system. By implementing standardised IT system, banks

can better mitigate the additional IT risks which stem from the cross border e-transactions. These risks involve the system compatibility and information integrity with the use of international telecommunication channels. However, banks have to also consider the additional country risk added to any cross border e-banking products. Local bank supervisors have to take the role of ensuring the local banks are incorporating the additional IT risks and country risk inherent in the cross border e-banking products within the overall bank's risk management. In addition, bank supervisors also have to monitor the possibility of increasing risks in the cross border e-banking transactions given the different country risks and the development of the global financial market conditions faced by the local banks.

5. Policy Recommendations

With the current state of IT implementation, the existence or non-existence of IT supervisory frameworks in SEACEN member countries, we can make some policy recommendations that can be workable with the coordinated efforts of the SEACEN countries. These recommendations are as follows:

1. Increase IT awareness by implementing and improving legal frameworks and promoting IT literacy amongst the financial society, financial institution managers and supervisors of financial institutions.

Despite the benefits of IT implementation for the general development of financial markets, IT risks still need to be managed to avoid potential financial instability resulting from IT failure. This should be done with the help of the financial society. Therefore, it is important to increase IT awareness by implementing and improving the legal framework to promote IT best practices in the SEACEN countries. IT literacy in the financial society is also a pre-requisite for good IT governance for financial institutions. The financial society with good IT governance practices will help mitigate IT risks in the financial markets.

2. Require banks/financial institutions to apply good IT governance by establishing IT supervisory frameworks referring to the best practices.

To minimise the probability of financial instability caused by IT failures in the financial institutions, authorities have to ensure that the practice of good IT governance in the financial institutions. The countries with more established IT supervisory frameworks mostly implement recommended risk-based management approach for the financial institutions. This approach still has to be supported by effective IT examination to verify their IT risks profile and

ensure banks provide adequate measures to mitigate the risks. Therefore, an IT supervisory framework has to be established and developed in line with the international standards and best practices. These standards and practices are always updated following the latest development in IT. Referring to these standards and practices will ensure the IT supervisory framework covers the potential development of IT implementation by financial institutions.

3. ***Promote coordination amongst financial institution supervisory authorities to have IT examination standards to bring all financial institutions within the country to the same level of IT risk management, therefore reducing potential systemic risks stemming from IT failure.***

In most countries, central banks are not the sole supervisory authority for all financial institutions. In Singapore, with the Monetary of Authority of Singapore being the sole authority of financial institutions, the model is much simpler compared to the practice in the U.S. with different authorities of financial institutions. The practice in the U.S. is similar to most SEACEN member countries. Therefore the establishment of a coordinated forum or organisation, such as the FFIEC in the U.S., is deemed necessary to create a uniform IT supervisory framework for all financial institutions. This uniform framework can help achieve the same standards of IT implementation for all financial institutions in the country.

4. ***Bringing IT implementation in SEACEN countries to a level playing field.***

IT implementation by financial institutions is beneficial for the management of the financial institution to help provide better and faster services, to support products and services research and development and to increase the quality of decisions by the management. However, the IT implementation by financial institutions should also be beneficial to the improvement of SEACEN financial markets. A level playing field is necessary in order to build an efficient and effective financial network amongst financial institutions in the region. A few recommended ways to achieve this are:

a) Increase knowledge sharing effort to design IT supervisory frameworks in all SEACEN member countries.

   IT supervisory frameworks need to be designed according to the level of IT implementation in the region and be reviewed and improved whenever it is necessary to control the IT risk stemming from the trend of IT implementation by financial institutions in the respective countries. However, the spillover effect from the more advanced countries in the region is expected to accelerate the learning process of the less developed countries. Better IT supervisory frameworks will lead to better standards of IT implementation by financial institutions;

b) Train bank supervisors / IT specialists to conduct effective IT audits, as well as provide career paths for IT specialists to retain experts in IT audits as part of bank supervision practices.

   The level of training should be done depending on the demand of the IT supervisory framework. Bank supervisors need to have basic knowledge of IT audit to be able to make a proficient assessment of IT risks in a financial institution. Whenever the framework demands for highly skilled IT auditors, IT specialists are needed to perform more detailed IT audit. In order to retain these skilled specialists, supervisory authorities should provide career paths with competitive remunerations compared to IT-specialised companies. These skills also need to be updated periodically to keep up with the latest IT developments.

References

BCBS (Basel Committee on Banking Supervision) 2001, "Risk Management Principles for Electronic Banking", Bank for International Settlements, May.

_____ 2003a, "Management and Supervision of Cross-Border Electronic Banking Activities", Bank for International Settlements, July.

_____ 2003b, "Risk Management Principles for Electronic Banking", Bank for International Settlements, July.

Federal Reserve Bank of Chicago, Information Technology Supervisory Resources, http://www.chicagofed.org/banking_information/information technology_ supervisory_resources.cfm

FFIEC (Federal Financial Institutions Examination Council), IT Examination Handbook, http://www.ffiec.gov

Greenspan, Alan, 2007, "The Age of Turbulence," *The Penguin Press HC,* September.

ITIL (Information Technology Infrastructure Library), http://www.itil.org

ISO (International Organization of Standards), http://www.iso.org

ISACA (Information System Audit and Control Association), COBIT 4.1 – Executive Summary and Framework, web site: http://www.isaca.org

_____, COBIT 4.1 – Brochure, web site: http://www.isaca.org

_____, Certified Information Security Manager (CISM) and Certified Information System Auditor (CISA), http://www.isaca.org

ISC^2 (International Information System Security Certification Consortium), Certified Information Systems Security Professional (CISSP), http://www.isc2.org

Katz and Shapiro, 1994, "Systems Competition and Network Effects," *The Journal of Economics Perspective,* Vol. 8, No. 2, (Spring), pp. 93-115.

Shapiro & Varian, 1998, "Information Rules: A Strategic Guide to the Network Economy," Harvard Business School Press, November.

Varian, 2005, "The Economics of Information Technology," Cambridge University Press, January 31.

PART 2: COUNTRY CHAPTERS

Chapter 2

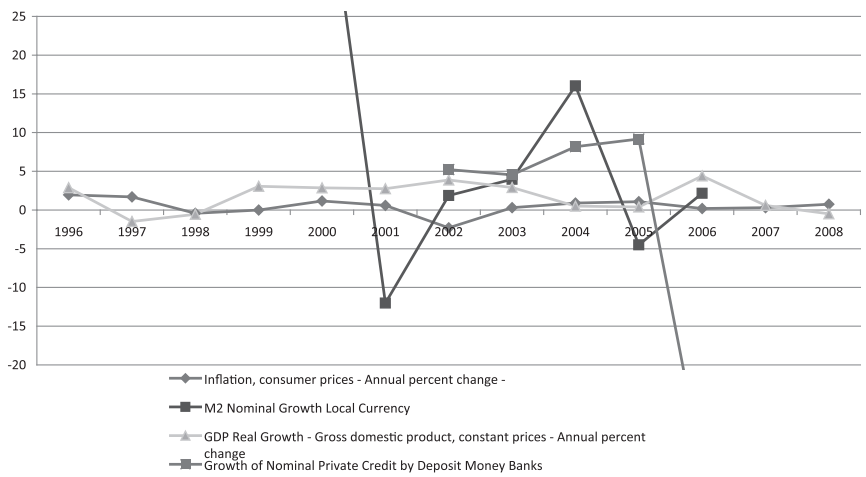
THE SUPERVISORY IMPACT OF TECHNOLOGY ON SEACEN FINANCIAL INSTITUTIONS: ISSUES AND CHALLENGES IN BRUNEI DARUSSALAM

by Zaki Mohidin[1]

1. Introduction

Brunei Darussalam is a small open economy, rich in natural resources, and dependent largely on oil and gas, with limited economic diversification. The oil and gas sector contributed, on average, about 67% of real GDP, 94% of Export earnings, and 91% of budget revenues during 2005-2007. Wealth from oil and gas provided the small population (estimated 398, 000 as of 2008, with over 30% of them below 19 years of age) with the highest standard of living (per capita GDP of $30,185 as of 2006) in Asia. While the overall GDP has grown by 1.0 % per annum during the past five years, oil and gas sector GDP has shown significant year to year fluctuations reflecting both technical variations in production and terms of trade fluctuations; and non-oil GDP has grown by about 5.0% per annum. With large current account and budgetary surpluses, and modest, but volatile, money and credit growth, inflation has remained subdued, averaging 1.0% (in terms of consumer price index) over the past five years.

Chart 1: Brunei— Select Economic Indicators, 1996–2008



Source: IMF World Economic Outlook and World Bank Financial Structure Database and World Development Indicators

1 Author is System Analyst of the Information Technology and State Store Department of Ministry of Finance, Brunei Darussalam.

2. Overview of the Financial System

Brunei Darussalam does not presently have a full-fledged central monetary authority or a central bank. All tasks related to fiscal and monetary issues are carried out by selected departments within the Government, under the jurisdiction of the Ministry of Finance (MOF) and the Prime Minister's Office (PMO) as follows:

- Issuance of currency – Brunei Currency and Monetary Board (BCMB);
- Monetary and exchange rate policy – (BCMB);
- Fiscal Management – Treasury Department, Revenue and Budget Sections (MOF)
- Reserve management – BCMB and Brunei Investment Agency;
- Financial sector supervision – Financial Institution Division (for domestic financial institutions), Brunei International Financial Centre (for offshore financial institutions) Ministry of Finance;
- Statistics – Department of Economic Planning and Development (DEPD), Prime Minister's Office and MOF;
- Research – BCMB; International and Research Division, MOF; and DEPD, Prime Minister's Office;
- Lender-of-last resort – This function has not been developed. However, BCMB may provide short-term standing facilities to the financial institutions against approved collateral.

The progression of financial institutions in Brunei Darussalam has been marked by significant growth over the last decade. This is demonstrated by the presence of a number of financial institutions of international standing and reputation, the advent of new financial instruments, the extensive nature of the financial transactions that are entered into and the numerous financial services that are now provided.

The relaxation of exchange controls and the development of Islamic institutions have also played their part in making the financial scene in Brunei Darussalam vastly different from what it was at the time of the passing of the Banking Act (Chapter 95), 1956.

The financial sector is based on a dual system whereby both conventional and Islamic financial products are readily available. Despite the small number of players in the Islamic financial sector, the growth of the sector has been rapid.

The domestic financial system can be divided into two categories:-

Banking System

- Commercial Banking
- Brunei Currency and Monetary Board (BCMB)

Non-Banking Financial Institutions

- Finance Companies
- Insurance Companies and Takaful
- Money-Changer and Remittances Business
- Employees' Trust Fund (TAP)
- Islamic Trust Fund of Brunei (TAIB)

Brunei Darussalam's development as an international financial centre began with the establishment of the Brunei International Financial Centre (BIFC). The BIFC is the licensing agency for off-shore companies including financial institutions such as banks, insurance companies and securities companies.

FINANCIAL SYSTEM STRUCTURE AS OF Q3 2008

FOR THE PERIOD TO Q3 2008	NO.	ASSETS	DEPOSITS	LOANS
Banks + TAIB	9	17.1 billion	13.6 billion	6.1 billion
Finance Companies	3	1.5 billion	897 million	1.2 billion
Offshore Banks	4	242 million	215 million	10 million
Retirement Fund	1	1.3 billion	1.2 billion	n/a

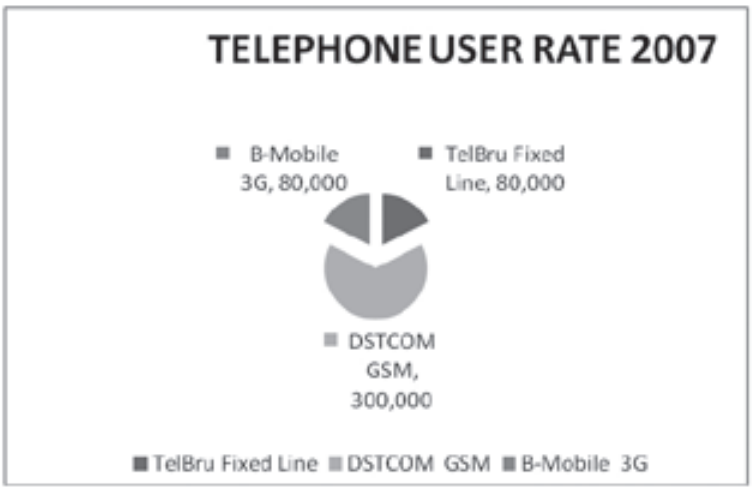
FOR THE PERIOD TO Q3 2008		ASSETS	GROSS PREMIUMS	GROSS CLAIMS
Insurance Companies & Takaful	13	1.1 billion	55.4 million	27.7 million
International Insurance Companies	1	202 million	23 million	n/a
Total Assets of Financial system				

FOR THE PERIOD TO Q3 2008		BUYING	SELLING	TOTAL REMITTANCE
Money Changers	27	78.4 million	82.4 million	n/a
Money Remittance + WU	25	n/a	n/a	368.7 million

	Jun-08
No. of ATM machines	155
No. of Banks	8 + 1 Trust Fund
No. of Branches	57

3. Survey of the IT Implementation

More than half of the population in Brunei Darussalam are Internet users, a steady increase of nine per cent over the previous year, according to 2007 figures from the Authority for Info-communications Technology of Brunei (AiTi). Brunei recorded a total of 199,532 Internet users in 2007, making up 50.8 per cent of the total population.



- *Are the following IT Infrastructure installed in the country?*

No.	Item	Yes/No
1	Communication Network	
	Cable (Phone line)	Yes
	Satellite	Yes
	Fiber Optic	Yes
2	Use of Cellular Phone	
	Is it relatively wide spread?	Yes
3	Use of Internet	
	Is it relatively wide spread?	Yes
4	National Payment System	No
5	Operated by government agency / central bank	No
6	Operated by an independent or private company (*Individual Banks*)	Yes
7	Automated/Computerised Payment System	Yes
8	RTGS	No
9	National Securities Settlement System	No

The payment and settlement system in Brunei Darussalam is not highly developed due to the small size of the local economy, population and low level of business volumes. In Brunei Darussalam, the absence of a central bank or monetary authority appears to have resulted in a well-preserved peer responsibility in the financial markets where players individually and collectively assist each other. It is predominantly the commercial banks which provide banking services ranging from basic payment and transfer services to remittances and serve the transaction needs of individuals and businesses in the economy. There are 8 commercial banks – 7 foreign and 1 local, which provide full banking services to the economy. Currently, there is no large value payment system and the main payment system consists only of a Clearing House (CH) which caters to retail or generally low value payments. The cheque clearing house is managed by a commercial bank namely, Hongkong and Shanghai Banking Corporation (HSBC) appointed for this purpose by the Brunei Association of Banks. Due to the smallness of Brunei Darussalam's banking market, the retail payment system is regarded as systemically important.

- *Are the following IT-related products implemented in the country?*

No.	Item	Yes/No
1	Credit Card	
	National (only used in the country)	Yes
	International	Yes
2	Debit Card	
	National (only used in the country)	Yes
	International	No
3	ATM	
	Individual bank	Yes
	Nationally-Shared ATM	No
	Internationally-Shared ATM	No
4	Electronic Fund Transfer (EFT)	Yes
5	EFT at Point of Sale	
	National (only within the country)	Yes
	International	Yes
6	Remittance Service	
	Domestic companies	Yes
	International companies	Yes
7	Phone Banking	
	Informational	Yes
	Transactional intra bank	Yes
	Transactional inter bank	No
8	Mobile/SMS Banking	

	Informational	Yes
	Transactional intra bank	Yes
	Transactional inter bank	No
9	Internet Banking	
	Informational	Yes
	Transactional intra bank	Yes
	Transactional inter bank	No
10	Pre-paid card	Yes

- *Regarding IT-related Applications in addition to IT-related products, are the following applications implemented with IT?*

No.	Item	Yes/No
1	Core Banking: General Ledger, Third Party Fund, Loan, and Consumer Information File	Yes
2	Treasury	Yes
3	Remittance	Yes
4	Trade Finance	Yes
5	Corporate Online Service	Yes

4. Impacts of IT Implementation on Financial Institutions

Larger banking institutions in Brunei Darussalam are always looking for the latest technological advancement in banking to attract new customers and maintain their market share. Although the country is mostly a cash society, with the introduction of online banking and cashless cards like credit and debit cards, more and more people are opting for the more convenient and efficient ways of making payments. With this in mind, the Electronic Transactions Act 2008 (ETA) was enacted which provides the legal framework for the "security and use of electronic transactions and for connected purposes". With the ETA, e-transactions will have legal effect and is equally enforceable in a court of law as those transactions conducted in the traditional manner.

- *IT Risks*

  As the impact of the level of IT Implementation in the country, what are the risks that need to be addressed and controlled in the financial system?

No.	Item	Yes/No
1	Operational Risk	Yes
2	Liquidity Risk	Yes
3	Credit Risk	Yes
4	Strategic Risk	Yes
5	Reputation Risk	Yes
6	Legal Risk	Yes
7	Compliance Risk	Yes

5. Prevailing IT Supervisory Framework and Regulations

The Financial Institutions Division (FID) is the supervisory arm of the Ministry of Finance, overseeing the financial institutions in Brunei Darussalam. Prior to the formation of FID, the supervision of financial institutions was undertaken by separate divisions under the Ministry of Finance. The Brunei Currency Board (now known as Brunei Currency and Monetary Board) was responsible for banking supervision and other financial institutions whilst the Economic Development Board was responsible for overseeing insurance activities.

Currently, the regulation of information technology in banking falls within the purview of the general supervisory and regulatory framework under the Banking Order 2006. Individual banks are responsible for managing and mitigating their IT risks which form part of the internal control environment which is integral to operational risk management of banks. While the business continuity plans and Disaster Recovery management by banks is evaluated and monitored offsite through one to one discussions between the FID and the CEOs of banks, IT system security and processes are assessed via the scrutiny of IT audit reports by internal, external and regional auditors of domestic and foreign banks.

- *Regarding IT supervisory framework,*

No.	Item	Yes/No
1	Is IT Implementation reported regularly?	No
2	Is IT audit conducted?	Yes
	By bank/IT supervisors from supervisory authority	No
	Off-site	No
	On-site	Yes
	By internal or external (third party) auditors (on-site)	Yes
	Special IT audit/examination outside regular examination (on-site)	No
3	Does the formal framework exist?	No
4	If yes, is it stipulated in a regulation?	
5	Is there minimum requirement in IT Implementation?	No
	Are the following items implemented: Active supervision by Top Management (IT Steering Committee)	Yes
	IT risk is included in the risk-based management	Yes
	System development life cycle	Yes
	All layers of IT system	
	Internal control system for IT Implementation	Yes
	Business Continuity Plan and Disaster Recovery Plan	Yes Yes
	Periodical IT audit (internal/external)	Yes
6	Because it involves supervision procedure, is IT outsourcing especially regulated?	No
7	Because it involves consumer protection, is E-banking products especially regulated?	No
8	Are any IT-related laws (cyber law, e-commerce, m-commerce, digital signature) installed?	Yes

- *Regarding on-site IT Audit,*

No.	Item	Yes/No
1	Is it conducted regularly?	No
2	If not regularly, is it conducted case by case?	No
3	If regularly, objects of audit:	
	Organization and Management	
	System development process	
	Operation	
	Software and Application, including E-Banking	
	Security (authentication, authorization and protection – including audit trails, encryption)	
	BCP/DRP	Offsite
	Communication Network	
	Outsourcing process	Offsite
	Internal Auditing	Onsite and offsite

6. Issues and Challenges

With the predominance of foreign banks of international repute in Brunei, the outsourcing of IT services by these banks has necessitated the development and implementation of IT oursourcing guidelines which have already been issued to all banks in Brunei which are required to apply for the approval of the Authority prior to outsourcing these activities as required by the provisions of the Banking Order.

Specific IT audits of banks will be conducted progressively as we build up capacity in this regard. There is currently insufficient skilled human resources for the supervision of IT systems. The Ministry lacks certified professionals, e.g., Certified Information Systems Auditor (CISA) to perform effective supervision on the IT systems in banks and financial institutions.

7. Suggested Policy

With the increasing use of technology in financial transactions by banks and other financial institutions, the integrity of IT dependent systems and processes is paramount. The overall policy framework of the Ministry of Finance would therefore ensure, through its Financial Institutions Division, that the payments and settlements system of the country which is facilitated by the commercial banks in Brunei will not be at risk under any circumstances. In the background of the

recent global financial crisis, the crisis management plan of the MOF ensures that all banks have developed their own crisis management plans within which, their Business Continuity Plan and Disaster Recovery management are two of the most critical elements. The MOF's policy is to ensure that all banks simulate various crisis scenarios and carry out crisis drills to test their individual plans to ensure that they can be depended upon when put into action.

The IT Department of the MOF should also complement the resources of the FID by building up their own capacity to carry out independent checks of the IT systems of banks and other financial institutions.

CHAPTER 3

THE SUPERVISORY IMPACT OF TECHNOLOGY ON SEACEN FINANCIAL INSTITUTIONS: ISSUES AND CHALLENGES IN CAMBODIA

by Hay Livine[1]
Sim Sothearith

1. Introduction

Financial institutions are rapidly increasing their use of technology to streamline operations, expand trading activities, improve service and minimise risks. In similar fashion, financial markets are eager to meet this challenge. The development of financial markets requires not only new products, new players and global rules, but also a robust financial infrastructure that can ensure efficient, secure and timely clearing, settlement and payment of financial transactions. Technology has been a major contributor to this development. Until recently, the growth in the volume of financial transactions was constrained by the physical burden of paper-based transactions and the capacity for communication. However, once information could be reduced to electronic form, large amounts of financial information as well as value could be processed and transmitted across markets. By linking local markets through networks, technology has created the global market. Towards this end, most central banks are beginning to introduce Real Time Gross Settlement (RTGS) inter-bank payment systems as the cornerstone of a modern electronic financial system.

Today, of course, nearly everyone uses ATM machines to get cash, deposit money, or transfer funds. There are banking products and services that are rapidly becoming more and more useful to busy people, such as mobile banking, which allows an account holder to check his balances, make transfers, view the transaction histories, and much more. Online banking offers customers the same services as mobile banking by allowing customers to access their accounts online through the Internet browser. Electronic banking (e-banking) can be done without cash or cheques. Customers can perform all these outside official hours after the bank has closed, including weekends. Electronic banking, then, is the delivery of banking products and services to customers through the electronic medium.

At the present, Cambodia has a poorly developed IT and technology infrastructure compared to other countries in the region. Cambodia is a country located in Southeast Asia that is bordered by Laos, Vietnam, and Thailand. Covering an area of about 181,035 square km, Cambodia is about half the size of

1 Authors are Section Chiefs of the Economic Research and Statistics Department of National Bank of Cambodia. The views and opinions represent in the paper are only of the authors and not those of the National Bank of Cambodia.

Vietnam. The capital of Cambodia is Phnom Penh and has the distinction of also being the largest city. The tenth largest river in the world, the Mekong River, is the longest river in Southeast Asia and the most important river in Cambodia. About 75% of the total population of around 14 million live in the rural areas and earn their living from agricultural product. GDP per capita was around US$512 in 2007 and the poverty rate was 35% according to the 2004 survey.

Cambodia was isolated from the international community during the period of the Cold War. With foreign-aid assistance of donors and NGOs, Cambodia went through rapid macroeconomic development over the last thirty years. In 1991, the United Nations Transitional Authorities (UNTAC) entered Cambodia to assist the nation conduct its first national election. The entry of UNTAC not only brought the country peace, but also computer literacy and a huge inflow of US dollar which transformed Cambodia into a dollarised economy.

Electronic banking, like ATM or e-banking, is something very new to the people in Cambodia. It is probably unheard of among those who live in the remote areas. This is due to the fact that Cambodia has low access to advance technology and it is partly due to the low level of English proficiency of the population. The use of computers is on the increase in Cambodia over the past decade and the trend is growing exponentially. Proficiency in English is now a pre-requisite for computer training. This requirement makes the training period very long for those who have not learned the language: the rural inhabitants, the children in school, and many government officials. Besides this, the banking sector, in particular, needs to be strengthened given its underdevelopment and its dominance in the present financial system.

This paper surveys the supervisory impact of technology on the financial institutions in Cambodia and evaluates the issues and challenges faced by the financial institutions in the implementation of financial IT-supported products and services. This paper also provides an overview of the recent developments of the financial institutions and their supervision by the National Bank of Cambodia.

The paper is divided into seven sections. Section 1 provides a broad description of the IT development in Cambodia. Section 2 discusses the financial system in Cambodia. Section 3 presents the findings of the survey on IT implementation. Section 4 reviews the impact of IT implementation on the financial institutions. Section 5 describes the prevailing IT supervisory framework and regulations. Section 6 addresses the issues and challenges. Finally, the policy recommendation is specified in Section 7. This research for this paper is based on secondary data as primary data is not available.

2. Overview of the Financial System

The National Bank of Cambodia (NBC), which was known as the Central Bank of Cambodia, was re-established in October 1979 and operated a mono-banking system through its provincial branches.

Khmer Riel (KHR) is the legal tender for Cambodia. In 1991, the first commercial bank (the Cambodia Commercial Bank or "CCB") was established under state joint venture for attracting investors and supporting the activity of the United Nations Transitional Authorities in Cambodia (UNTAC). In late 1991, Cambodia converted from a planning economy to a free market economy and transformed its banking system from a mono-banking system to a two-tiered banking system.

The state liberalised the banking sector allowing for the establishment of commercial banks and the operation of foreign bank branches under local laws. This made it necessary for the National Bank of Cambodia to strengthen its capacity in bank regulation and supervision through the promulgation of laws and regulations.

As a result, the new central bank act was promulgated in January 1996 to establish clearly the authority, ownership and capital structure of the NBC, and laying a more solid foundation for its operations. To further strengthen the banking system, the National Bank of Cambodia introduced a bank-restructuring programme in early 2000, requiring the commercial banks to increase their capital base and to comply with the relevant laws and regulations. Since then the number of banks and branch network have expanded, making the banking business more competitive.

The increase in the number of banks and bank branches in the provinces and cities, and the modernisation of banking products and bank services, such as ATM, Internet banking, credit cards, debit cards, wire transfer, and other modern services, served the needs of the public, resulting in a rapid expansion of the banking sector. The expansion of banking activities can also be seen through the increase in the total assets of the banking system from KHR 3,799 billion in 2003 to KHR 13,445 billion in 2007, reflecting a sharp increase of 254% over the period of five years. The rapid growth of the banking sector resulted in a jump in the ratio of total bank assets to the GDP to 41% compared with the average ratio of 21% over the last 5 years.

The four largest banks held 64% of the net asset of the banking system as at the end of 2007. This figure indicates a heavy concentration and heterogeneity in the Cambodian banking system.

Figure 1
Total Assets to GDP

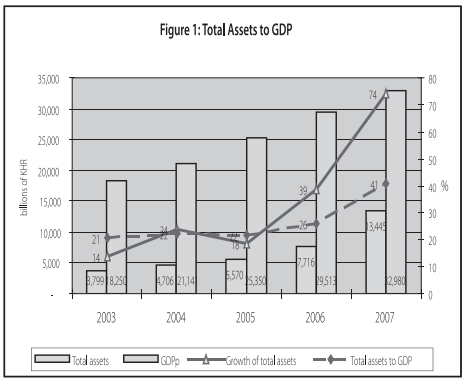


Figure 2
Component of Assets

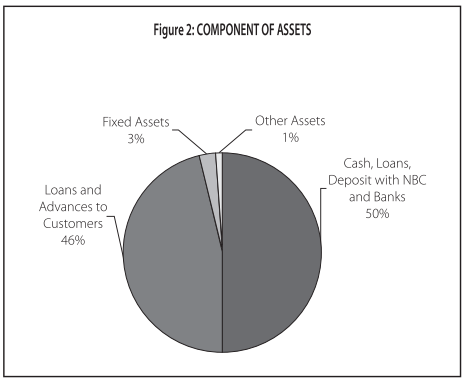


Figure 3
Comparison of Total Assets

	2007	Share	2006	Share	2005	Share	2004	Share	Growth Rate (%) 2007 over 2006	2006 over 2005
Commercial Banks										
1 Cambodian Public Bank	2,260,384	16.8%	983,973	12.8%	664,392	11.9%	575,352	12.2%	129.7%	48.0%
2 Canadia Bank Plc.	2,242,342	16.7%	1,622,672	10.7%	1,226,574	22.0%	1,072,066	21.5%	47.3%	24.2%
3 ANZ Royal Bank (Cambodia) Ltd.	2,241,988	16.7%	830, 301	10.8%	370,364	6.6%	-	0.0%	170.0%	124.2%
4 Acleda Bank Plc.	1,899,200	14.1%	900,576	11.7%	508,287	9.1%	338,154	7.2%	110.9%	77.2%
5 Foreign Trade Bank of Cambodia	862,067	6.6%	806,400	11.6%	673,701	12.1%	663,361	14.1%	1.6%	33.1%
6 Cambodian Commercial Bank Ltd.	651,741	4.8%	519,549	6.7%	460,263	8.3%	479,072	10.2%	25.4%	12.9%
7 May Bank, Phnom Penh Branch'	579,078	4.3%	339,710	4.4%	271,471	4.9%	270,230	5.7%	70.5%	25.1%
8 Vattanac Bank Ltd.	525,000	3.9%	207,090	0.7%	220,540	4.0%	160,014	0.4%	82.7%	30.3%
9 Union Commercial Bank Plc.	464,253	3.6%	423,585	5.5%	348,760	6.3%	405,206	8.6%	14.3%	21.4%
10 Krung Thai Bank Public Co. Ltd. P.P. Branch*	286,990	2.1%	203,423	2.6%	203,342	3.7%	201,353	4.3%	41.1%	0.0%
11 Cambodia Mekong Bank Public Ltd.	240,074	1.0%	109,339	1.4%	88,076	1.0%	02,083	1.0%	127.4%	24.1%
12 First Commercial Bank, Phnom Penh Branch*	239,441	1.8%	210,930	2.7%	164,916	3.0%	174,630	3.7%	13.5%	27.9%
13 Singapore Banking Corporation	195,825	1.5%	150,816	2.0%	127,163	23%	117,037	2.5%	29.8%	18.6%
14 Advanced Bank of Asia Ltd.	100,104	1.2%	111,703	1.4%	87,015	1.0%	98,709	2.0%	46.0%	28.4%
15 Shinhan Khmer Bank	146,180	1.1%	-	0.0%	-	0.0%	-	0.0%	0.0%	0.0%
16 Cambodia Asia Bank Ltd.	129,027	1.0%	89,856	1.2%	72,187	1.3%	60,968	1.3%	43.6%	24.5%
17 CAMKO Bank Ltd.	94,792	0.7%	-	0.0%	-	0.0%	-	0.0%	0.0%	0.0%
Sub-total	13,270,210	98.7%	7,580,296	98.2%	5,486,775	98.5%	4,634,884	98.5%	75.1%	38.2%
Specialized Banks										
18 Rural Development Bank	79,534	0.5%	65,195	0.8%	53,703	1.0%	43,739	0.9%	12.8%	21.4%
19 First Investment Specialized Bank	28,623	0.2%	26,938	0.3%	-	0.0%	-	0.0%	6.3%	0.0%
20 Specialized Bank Peng Heng S.M.E Ltd.	20,503	0.2%	16,909	0.2%	16,167	0.3%	15,074	0.3%	21.3%	4.6%
21 Prosperity Investment Specialized Bank Plc.	18,771	0.1%	-	0.0%	-	0.0%	-	0.0%	0.0%	0.0%
22 Cambodia Agriculture Industrial Specialized Bank	12,788	0.1%	15,684	0.2%	12,997	0.2%	12,505	0.3%	-18.5%	20.7%
23 Anco specialized Bank	10,688	0.1%	11,030	0.1%	-	0.0%	-	0.0%	-3.1%	0.0%
24 Cambodia Development Specialized Bank	9,986	0.1%	-	0.0%	-	0.0%	-	0.0%	0.0%	0.0%
Sub-total	174,893	1.3%	135,757	1.8%	82,867	1.5%	71,317	1.5%	28.8%	63.8%
Total	**10**,445,100	100.0%	7,718,050	100,0%	5,580,842	100.0%	4,708,202	100.0%	74.4%	00.5%

*** Foreign branches**
Note. All figures are unaudited and as reported by banks

As part of the implementation of the Law on Banking and Financial Institutions, the banking system was restructured. At the end of 2007, the banking system of Cambodia consisted of the National Bank of Cambodia, 17 commercial banks (three foreign bank branches), seven specialised banks (of which one is state-owned), 17 licensed microfinance institutions and 23 registered microfinance institutions. (See Figure 4 below).

Figure 4
Number of Offices of Banks and MFIs

		Phnom Penh[1]			Prvincial		
	TotaL	Branch	Sub-branch	Money changer	Branch	Sub-branch	Money changer
Commercial Bnaks							
1 Acleda Bank plc.	102	9			23	70	
2 ANZ Royal bank (Cambodia)Ltd..	16	8			5	3	
3 Canadia Bank Plc	15	4			11		
4 Singapore Banking Corporation	14	2		7	1		4
5 Cambodia Asia Bank Ltd.	14	1		6			7
6 Cambodian Public bank	11	6			5		
7 Cambodia Mekong Bank	7	4		1	2		
8 Union Commercial Bank	4	1			3		
9 Cambodian Commercial Bank	4	1			3		
10 Advanced Bank of Asia Ltd.	3	1			1		1
11 Vattanac Bank Ltd.	2	1			1		
12 Krung Thai Bank Public Co.Ltd., PP Branch*Vattanac Bank Ltd.	2	1			1		
13 May Bank, Phnom Penh Branch*	2	1	1				
14 First Commercial Bank, Phnom Penh Branch*	1	1					
15 Foreign Trade Bank of Cambodia	1	1					
16 Camko Bank Ltd.	1	1					
17 Shinhan Khmer Bank	1	1					
Total	***200***	***44***	***1***	***14***	***56***	***73***	***12***
Specialised Banks							
18 First Investment Specialised Bank	1	1					
19 Cambodia Agriculture Industrial Specialised Bank	2	1			1		
20 Anco Specialized Bank	1	1					
21 Rural Development Bank	1	1					
22 Specialised Bank Peng Heng S.M.E Ltd.	1	1					
23 Prosperity Investment Specialised Bank	1	1					
24 Cambodian Development Specialised Bank	1	1					
Total	***8***	***7***	***0***	***0***	***1***	***0***	***0***
Microfina nce Institutions							
1 PRASAC	115	1			14	100	
2 Cambodia Enterprenur	103	1			11	91	
3 Angkor Microherhvatho Kampuchea	97	1			13	83	
4 AMRET	88	1			16	71	
5 Thaneakea Phum Cambodia	87	1			9	77	
6 Hattakasekar	79	1			7	71	
7 CREDIT	70	1			7	62	
8 Vision Fund Cambodia	62	1			8	53	
9 SEILANITHIH	47	1			6	40	
10 Enten Akpevath Pracheachun	28	1			8	19	
11 CHC	26	1			5	20	
12 Cambodia Business Intergrate in Rural Development	21				6	15	
13 MAXIMA	16	1			2	13	
14 Tong Fang Microfinance	16	1			2	13	
15 Intean Poalroath Rongroeung	16	1			5	10	
16 Pisit Akphiwat Sethakeh	6				2	4	
17 Famer Union Development Fund	5	1			1	3	
Total	***882***	***15***	***0***	***0***	***122***	***745***	***0***

* Foreign Branches

[1] Including head office

To satisfy their clients, banks and financial institutions seek to design and develop new and innovative financial products in terms of faster product delivery, speedier access to financial services and lower costs. In view of the introduction of electronic banking in banks and financial institutions in Cambodia and use of IT in the banking sector, it is important to establish a regulatory framework for electronic banking to protect depositors. The risks associated with electronic banking include all the inherent banking risks. The National Bank of Cambodia is in the process of holding discussions with the banks and financial institutions and is working towards the establishment of a regulatory framework on e-banking to ensure the safety of depositors' funds.

Figure 5
Terminals, ATM Cards, Debit Cards and Credit Cards
As at December 31, 2007

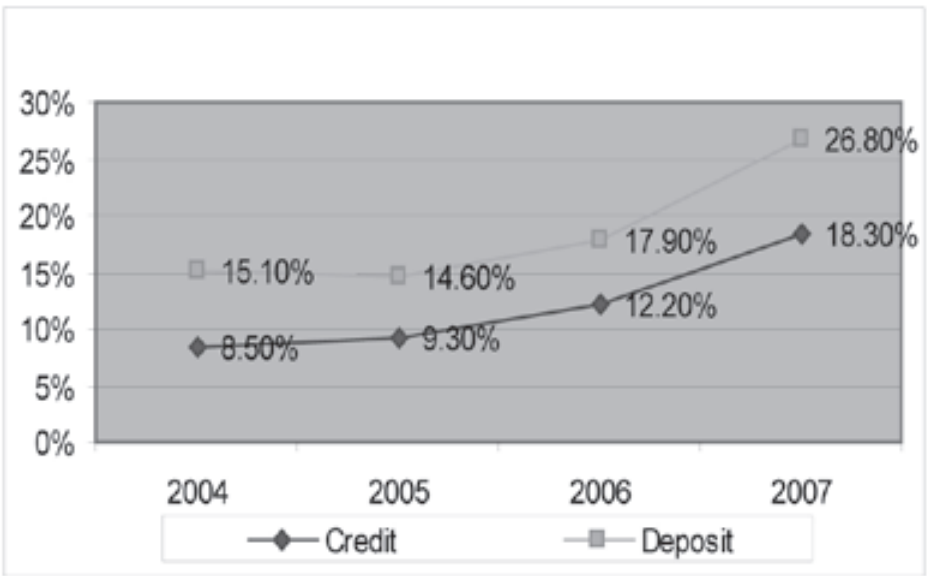
	ATM terminals	ATM Cards	POS **	Debit Cards	Credit Cards
Commercial Banks					
1 Alcleda Banks Plc.	23	-		56,615	-
2 Advanced Bank of Asia Ltd.	-	-		-	-
3 ANZ Royal Bank (Cambodia) Ltd.	91		582	64,870	-
4 Cambodia Asia Bank Ltd.	-	-		-	-
5 Cambodia Mekong Bank Public Ltd.	2	-	383	-	332
6 Cambodian Commercial Bank Ltd.	-	-		-	-
7 Cambodian Public Bank Ltd.	13	3,477	120	-	-
8 Canada Bank Plc.	25	-	510	12,615	2,317
9 First Commercial Bank, Phnom Penh Branch*	-	-		-	-
10 Foreign Trade Bank of Cambodia	-	-		-	-
11 Krung Thai Bank Public Co. Ltd. P.P. Branch*	-	-		-	-
12 May Bank, Phnom Penh Branch*	-	-		-	-
13 Singapore Banking Corporation Ltd.	4	-	5	7,330	1,349
14 Union Commercial Bank Plc.	5	-	67	450	955
15 Vattanac Bank Ltd.	7	718		2,200	-
16 Camko Bank Ltd.	2			238	
17 Shinhan Khmer Bank					
Sub-total	172	4,195	1,667	146,351	4,953
Specialized Banks					
18 Anco Specialized Bank Ltd.	-	-		-	-
19 Cambodia Agriculture Industrial Specialized Bank	-	-		-	-
20 First Investment Specialized Bank Ltd.	-	-		-	-
21 Rural Development Bank					
22 Specialized Bank Peng Heng S.M.E. Ltd.	-	-		-	-
23 Prosperity Investment Specialized Bank	5				
Sub-total	5	-		-	-
Total	**177**	**4,195**	**1,667**	**146,351**	**4.953**

** Foreign branches*

*** Point of Sale terminal*

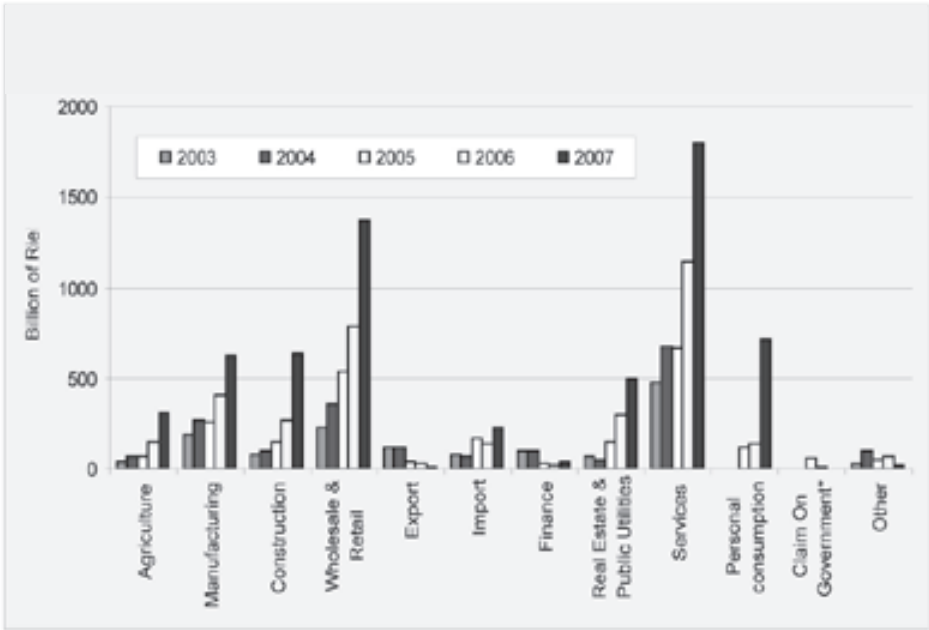
The development of financial services is good news for both consumers and investors. However, these services are associated with risks that need to be monitored and supervised to safeguard deposits and the system as a whole. In this sense, the National Bank of Cambodia has a crucial task for preventing financial institutions from engaging in high-risk transactions through prudential regulation and the enforcement of laws. By the end of 2007, the total credit granted to customers amounted to KHR 6,335 billion (US$1,582 million), an increase of 77% compared to 2006 when total credit was KHR 3,579 billion (US$ 882 million). Credit to GDP went up to 18.3% in 2007, while the ratio was 12.2% in 2006 and only 8.5% in 2004. Deposits to GDP rose from 17.9% in 2006 to 26.8% in 2007.

Figure 6
Credits and Deposits to GDP



The economic sectors that benefited from bank lending include the services sector, with an increase by 57%, the wholesale and retail sector by 75%, the real estate and public utilities by 65%, the industrial sector by 52%, and the construction sector by 138%. This increase was in line with the economic growth of 9.6% in 2007. Services, wholesale and retail sectors remained the sectors that benefited from the highest market share.

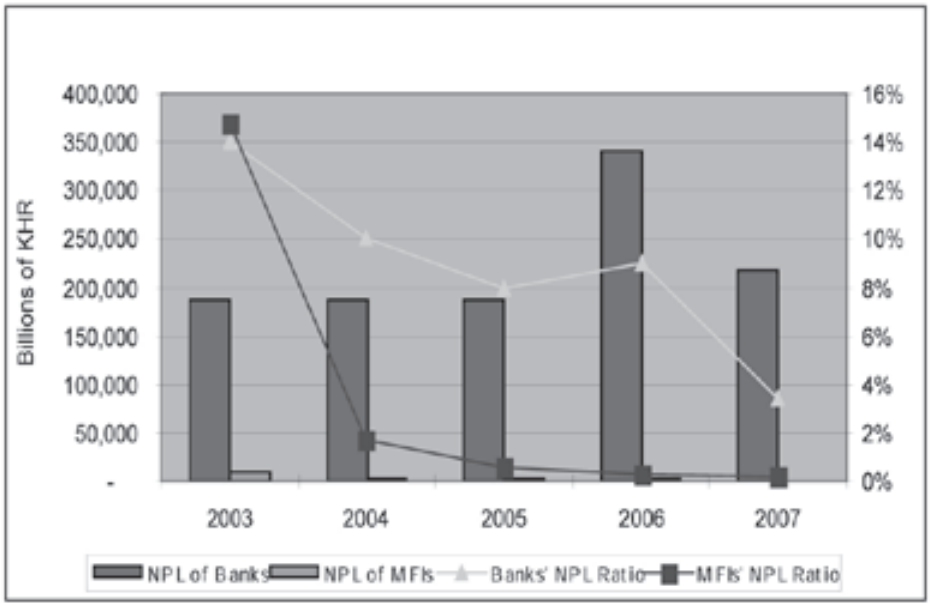
Figure 7
Loans by Sectors



Such a rapid increase in lending has never been recorded before in Cambodia. At the same time, Non-Performing Loan (NPLs) of the banking sector remained at their lowest level of 3.4% and as low as 0.2% among the microfinance institutions. This raises some concerns for National Bank of Cambodia, particularly as to accuracy of loan classification and the transparency of the decision-making process. Another issue is that the ratio of general provision to total loan decreased from 0.8% in 2006 to 0.7% in 2007, despite the increase in lending.

2007's insolvency ratio of 23.57% exceeds the required minimum of 15%, but it is lower than in the previous year due to the increase in loans and advances. Because of the amendment in the Prakas on the calculation and control of large exposure in 2005 (mainly in the way risks are weighted,) and the tightening of large exposure supervision, large exposure lending decreased from its highest level of 90.4% in 2005 to 9.13% in 2007. The implementation of prudential regulations is aimed at maintaining a safe and sound banking system. The main prudential regulations include: non-performing loans, loans to related party, large exposure loans, and capital adequacy.

Figure 8
Non-performing Loans of Banks and MFIs



The Credit Information System (CIS) is an important tool in the loan approval process which can aid rural credit growth, especially when there is intense competition between microfinance institutions in this sector. Thus, the absence of a CIS for microfinance institutions is considered a drawback that causes the level of lending growth to be low and limits participation in the rural credit sector. According to the Financial Sector Development Strategy 2006-2015, the credit information system established for the commercial bank sector can be extended to the microfinance sector.

3. Survey of IT Implementation

Today, information of all kinds is transmitted easily, inexpensively and instantaneously around the world, providing finger-tip access to anyone with a laptop computer, cellular phone or palm pilot. As an example, the most popular items on the Federal Reserve's public web site – including statistical reports on foreign exchange rates, selected interest rates, consumer credit and industrial production, along with press releases and Federal Open Market Committee announcements – are accessible by wireless remote. The growing importance of the Internet as a distribution channel is also eroding the traditional barriers between financial service providers and technology firms. Banks are increasingly providing technology services, such as account reconciliation software and "web-enabling" assistance, while technology firms are making inroads into services once the domain of banks and brokerage firms, such as financial planning and

bill payment. Indeed, many banks are beginning to think of technology firms as competitors or are contemplating ways to partner with them.

Cambodia in particular, lacks infrastructure and computer knowledge so Internet use is limited. English language proficiency is also a problem. Today, Cambodians are beginning to use modern technology in their everyday lives. Shiny new cars shuttle Cambodians across the country in a few hours, a journey which once took days. Mobile phones allow cheap and reliable communication with loved ones far away, and digital cameras can make a permanent record of memorable moments. However, it is computers that have the potential to revolutionise Cambodian society. Arguably the most important development, and certainly the most popular, is the Internet. As a worldwide network, the Internet links Cambodians to the global community, allowing it to understand what is happening around the world quickly and easily. Although few Cambodians are computer literate and Internet availability is limited, the Internet is already beginning to change Cambodia for the better. According to statistics, there were only 6,000 Cambodian users in 2000. This figure has since increased to 44,000 Cambodian users which is equal to 0.3% of the population. This means that the number of Internet users in Cambodia is still low, although Internet providers are heavily investing in the sector. Statistics from the Ministry of Post & Telecommunication indicate that, between 2000 and 2003, there were only 159 Internet cafés nationwide.

Although the Internet opens the door to a wealth of information and communication, allowing quicker, more efficient work, the service is currently beset with difficulties. Fast and reliable Internet connections are usually dependent on advanced infrastructure so, although most schools and universities in Phnom Penh have Internet access, the story is very different in provincial Cambodia. In rural areas, many do not even have access to electricity. There are now 7 ISPs in Cambodia, namely, Camnet, Bigpond (CogeTel), Open Forum, CaminTel, Telesurf, Camshin, and Casacom. Broadband Internet services are now being provided through ADSL wireless service or optic fiber in Phnom Penh. Optic fiber cable was installed from Thailand to Vietnam through a route of some Cambodian's provinces. In addition, a loan agreement for "Greater Mekong Telecommunication Backbone Network Project (Cambodia Growth Corridor)" was signed in March 2005 between the Cambodian Government and JBIC and a project to install the total length of 400km of optic fiber cable connecting some provinces within Cambodia has already started.

Figure 9
Status of Installed IT Infrastructure

Are the following IT Infrastructure installed in the country?

No.	Item	Yes/No
1	Communication Network	Yes
	Cable (Phone line)	Yes
	Satellite	Yes
	Fiber Optic	No
2	Use of Cellular Phone	Yes
	Is it relatively wide spread?	Yes
3	Use of Internet	Yes
	Is it relatively wide spread?	No
4	National Payment System	No
5	Operated by government agency / central bank	No
6	Operated by an independent or private company	No
7	Automated/Computerised Payment System	No
8	RTGS	No
9	National Securities Settlement System	No
	Operated by government agency / central bank	No
	Automated/Computerised Settlement System	No

Figure 10
Status of Installed IT Infrastructure

Are the following IT-related products implemented in the country?

No.	Item	Yes/No
1	Credit Card	Yes
	National (only used in the country)	Yes
	International	Yes
2	Debit Card	Yes
	National (only used in the country)	Yes
	International	No
3	ATM	Yes
	Individual bank	Yes
	Nationally-shared ATM	No
	Internationally-shared ATM	No
4	Electronic Fund Transfer (EFT)	Yes

5	EFT at Point of Sale	Yes
	National (only within the country)	Yes
	International	No
6	Remittance Service	No
	Domestic companies	No
	International companies	No
7	Phone Banking	No
	Informational	No
	Transactional intra bank	No
	Transactional inter bank	No
8	Mobile/SMS Banking	No
	Informational	No
	Transactional intra bank	No
	Transactional inter bank	No
9	Internet Banking	Yes
	Informational	Yes
	Transactional intra bank	Yes
	Transactional inter bank	No
10	Pre-paid card	Yes

Figure 11
Status of IT-related Applications in Addition to IT-related Products

Regarding IT-related applications in addition to IT-related products, are the following applications implemented with IT?

No.	Item	Yes/No
1	Core Banking: General Ledger, Third Party Fund, Loan, and Consumer Information File	No
2	Treasury	No
3	Remittance	No
4	Trade Finance	No
5	Corporate Online Service	No

4. Impact of Impact of IT Implementation on Financial Institutions

4.1 Operational Risk

Specific areas related to operational risks in the country:

1. The bank becoming a target for money laundering.
2. The growth in e-commerce, e-fund transfer, mobile banking, and Internet banking potentially pose significant operational risks for both consumers and banks (e.g., fraud and system security issues).
3. Any country events, such as elections, neighboring dispute, economic recession/depression, etc., that could bring disruptions to business activities in the country.

4.2 Risks and Impact of IT Implementation

Risks and impact of the IT implementation on financial institutions:

1. Programming errors:
   e.g., good data is processed by incorrect programmes (applications).
2. Processing errors:
   e.g., transactions are incorrectly processed more than once against the same master file that cause temporary disruptions to system.
3. Data and database management errors:
   e.g., inadequate (poor) management of the systems maintenance process, such as providing users access to unlimited (not specific) data or database within the environment.
4. Physical damage:
   e.g., devices unprotected from damage, theft and inappropriate uses, hijacking of the data system, or virus attack

4.3 Types of IT-related Risks

Figure 12
Types of IT-related Risks

As to the impact of IT Implementation in the country, what are the risks that need to be addressed and controlled in the financial system?

No.	Item	Yes/No
1	Operation Risk	Yes
2	Liquidity Risk	Yes
3	Credit Risk	Yes
4	Strategic Risk	Yes
5	Reputation Risk	Yes
6	Legal Risk	Yes
7	Compliance Risk	Yes

Insights on IT risk reductions by the supervisory framework at country level:

1. Lacking IT technical resources is the weakness. This should be strengthen at the education level rather than alone at organisation level (technical risk).
2. The supervisory procedure seems to be invisibly carried out along with the existing regulations (compliance risk & legal risk).

5. Prevailing IT Supervisory Framework and Regulations

Figure 13
Status of IT Supervisory Framework

No.	Item	Yes/No
1	Is IT Implementation reported regularly?	Yes
2	Is IT audit conducted?	Yes
	By bank/IT supervisors from supervisory authority	Yes
	Off-site	No
	On-site	Yes
	By internal or external (third party) auditors (on-site)	Yes
	Special IT audit/examination outside regular examination (on-site)	Yes
3	Does the formal framework exist?	No
4	If yes, is it stipulated in a regulation?	
5	Is there minimum requirement in IT implementation?	Yes
	Do the following items implemented: Active supervision by Top Management (IT Steering Committee)	Yes
	IT Policy and Standard Operating Procedure	Yes
	IT risk is included in the risk-based management	Yes
	System development life cycle	Yes
	All layers of IT system	Yes
	Internal control system for IT Implementation	Yes
	Business Continuity Plan and Disaster Recovery Plan	Yes
	Periodical IT audit (internal/external)	Yes
5	Because it involves supervision procedure, is IT outsourcing especially regulated?	Yes
6	Because it involves consumer protection, ise-banking products especially regulated?	Yes
7	Are any IT-related laws (cyber law, e-commerce, m-commerce, digital signature) installed?	No

Countries such as Germany, Switzerland, US, and Singapore are the main reference points in the designing of the supervisory framework in Cambodia. But some banks do not have IT supervisor, however, in controlling IT risk, we have Business Support Team, BCP Committee in IT Division, decision-making level IT Management Committee (ITMC) which is supported by BST, and the BoD level of Audit Risk Committee (ARCO), chaired by BoD member, to control the overall banking risk including IT Risk.

We control IT risks by our risk management committee and also by a special audit team when we suspect the presence of any risks.

Figure 14
Status of IT Audit

No.	Item	Yes/No
1	Is it conducted regularly?	Yes
2	If not regularly, is it conducted case by case?	
3	If regularly, objects of audit:	
	Organisation and Management	Yes
	System development process	Yes
	Operation	Yes
	Software and Application, including e-Banking	Yes
	Security (authentication, authorisation and protection – including audit trails, encryption)	Yes
	BCP/DRP	Yes
	Communication Network	Yes
	Outsourcing process	Yes
	Internal Auditing	Yes

The NBC has plans for capacity building and intends to send its bank supervisors and IT auditors for training overseas.

6. Issues and Challenges

6.1 Issues

- Cambodia is presently in the early stage of IT development. Its IT capacity building is very limited as compared to the neighboring countries. Thus, more development in IT infrastructure and IT legal framework is needed.

- Insufficient qualified IT staff to conduct IT supervision.

- Lack of IT auditing firms.
- Lack of IT standards for banking and financial institutions to implement.
- Low level of awareness of IT-related products and IT-related risks.
- Law on banking and financial institutions not yet cover IT supervision.

6.2 Challenges

- Lack of financial resources is the major concern in the building up of IT infrastructure.
- ATM networks are proprietary, owned by individual banks. Customers would like banks to operate a nationally shared ATM network.
- Individual banks have to the responsibility to assess, identify, and mitigate the risks associated with IT implementation and IT-related products. The National Bank of Cambodia only conducts on-site and off-site examination.
- Application and implementation of IT is new to Cambodia. Lacking experience and expertise in the management of IT-related risks and supervision, the banking system is susceptible to cyber crime.
- One of the challenges to Cambodia is bringing all banks together into a common payment system because most of the settlements are still transacted in cash.

7. Policy Recommendations

Cambodia imports every IT technology and IT system equipment. The banking and financial institutions, including the National Bank of Cambodia, should monitor their own IT systems to mitigate the risks, by increasing IT risk awareness among top management, monitoring and collecting information from within and outside the country on IT risk-related matters and learn from the lessons of experience.

In addition, Cambodia or The SEACEN Centre should conduct workshops twice a year on the management of IT risks associated the implementation of IT in the banking and financial sector. It will be to the mutual benefit of SEACEN member countries for the central banks to update and share the member banks' country experience.

References

Master Plan for Implementation of Open Source in Cambodia, 25 February, 2005 < www.nida.gov.kh/activities/foss/pdf/MasterPlanFOSS.pdf >.

Department of Banking Supervision, National Bank of Cambodia, "Annual Report 2005, 2006 & 2007".

Schaechter & Andrea, "Challenges of the E-banking Revolution," *Finance & Development ,* 1 September, 2002.

Risk Management Principles for Electronic Banking, Report from Bank for International Settlements, May 2001.

Cambodia Internet Usage and Telecommunications Reports <http//www.internetworldstats.com/asia.kh.htm>

Joseph Yam, (1998), "The Impact of Technology on Financial Development in East Asia," *Journal of International Affairs*, Vol. 51.

The Impact of Today's Technology on Banking and the Financial Markets, Report at the Eleventh International Conference of Banking Supervisors, 20 September, 2000.

Tharman Shanmugaratnam, Challenges Of The New Financial Landscape: Emerging Trends and Implications for Regulation, Report at the 4th Law Asia Business Law Conference, 3 November, 2000.

CHAPTER 4

THE SUPERVISORY IMPACT OF TECHNOLOGY ON SEACEN FINANCIAL INSTITUTIONS: ISSUES AND CHALLENGES IN INDONESIA‡

by Cicilia A. Harun[1†]

1. Introduction

Indonesia is known as a nation that embraces technology development. It adopts the use of communication and computer technology quickly as part of its everyday life. In regard to communication technology, the use of cellular phones has been widespread reaching even the lower income class. If not for the relatively high cost of personal computers and of the Internet connection, the use of the Internet would have been extensive. The financial sector has taken advantage of the strong appetite for innovation to proliferate the market with products using the latest technology available. This has to be anticipated by the financial authorities to insure the integrity of the financial system and to safeguard the stability of the financial system. Although cyber crime is not yet a major concern in Indonesia, some security issues of the technology-supported payment system have surfaced. Implementation of information technology poses risks from the potential failure of the system in conjunction with the dependence of financial institutions on the system. There is a concern in striking a balance between the use of technology for financial products and operations and the effort needed to safeguard the integrity of the financial system. The latter should be the first priority. However, it is also important to let the financial system evolve using the latest technology available, while maintaining the prudential principles.

The dual role of technology allows financial institutions to tap into a wider range of customers and clients, therefore diversifying markets. The customers and clients of the financial institutions also benefit from the economies of scale associated with the implementation of IT in the form of reduced fee per transaction and account. Because of the potential efficiency gain, the financial institutions will seek out the more advanced technology to implement in order to support their operation as well as to develop financial products. For this reason, financial institution supervisors should never fall behind in learning the latest technology that can be implemented in the financial world.

1‡ The views and opinions expressed in this paper are solely that of the author. They do not represent the policy or stance of Bank Indonesia. Some of the material is excerpted from Bank Indonesia's IT supervisory framework and the regulation for IT implementation by commercial banks, issued by the Directorate of Banking Research and Regulation and Directorates of Banking Supervision. This version is presented in the first workshop of the SEACEN Research Project "The Supervisory Impact of Technology on SEACEN Financial Institutions: Issues and Challenges" as a preliminary country paper.

† Researcher at the Financial System Stability Bureau, Directorate of Banking Research and Regulation, Bank Indonesia, email: charun@bi.go.id. The author would like to thank Ida Rumondang at Bank Indonesia for the valuable input and guidance provided in the discussion of the material.

In addition to the dual role of technology in providing benefits to the financial institutions, the implementation of technology in general also create the network effects. Technology simplifies the procedure in acquiring financial services. Financial service users tend to prefer a system that can give them the easiest and widest access to their counterparties. Users will assess the inherent and network values of joining the system network and make their choices accordingly. For the potential market reach, financial institutions always strive to provide the highest value of network externalities by implementing the state-of-the-art technology.

With the increasing role of technology in the financial institutions and markets, financial institutions now have to integrate the technology risk in their overall operational risk. Financial institutions need to be cautious with the possibility of technology failure that can adversely affect their business operation, causing financial and opportunity loss as well as damaging their reputation. In addition, they also have to safeguard the security of data, since they maintain sensitive financial data and customers/client's information. Protecting the security of the data becomes a major part of the development of technology implemented in financial institutions. The more complex the technology implemented in the operation of the financial institution, the higher the technological skill that is required of a financial institution supervisor (FIS) in order to do a good job in supervising the financial institution. Nevertheless, there exist today financial institution supervisors who are certified information technology (IT) auditors, dedicated to the auditing of the technology systems of financial institutions.

On the positive side for the FIS, the use of technology in the operation of financial institutions also makes operational errors easier to measure. Before technology dominates the operation of the financial institution, operational risk was always hard to measure. Nowadays, the financial institutions can measure operational risk by categorising transaction errors according to the monetary cost potentially spent to correct the errors, and can easily count the frequency of the transaction errors for each category and arrive at the overall monetary cost for transaction failures. The application of technology also makes it easier to establish the traceability of transactions. Some transactions can be categorised as HFLI (high frequency low impact), and the rest can be categorised as LFHI (low frequency high impact). A secured IT system detects operational fraud easily, forcing people to think twice before misusing the system. On the negative side, a FIS has to understand the entire mechanism of the financial product offered by the financial institution in order to determine whether the operation is compliant to the law and regulation. The process of understanding the product requires the FIS to know of how the technology works, and to possess the skill in certain cases to provide recommendation in promoting best practices. The implementation of IT in financial institutions also allow transactions to be executed in a manner of seconds, leaving no time for verification of the possibility of money laundering

or other forms of illegal transactions. The capability of a FIS to do technology auditing within the system development life cycle is then challenged with the rapid-growing use of technology in financial institutions.

The rationale of technology implementation by financial institutions tells us that the use of technology in financial institution is something that should be embraced and not discouraged. Nevertheless, the top priority of the FIS should be the sustainability of the financial institution, if not the overall financial stability. The implementation of technology should follow the fulfillment of well defined prerequisites. This is to make sure that the financial institution gains nothing but all the benefits from the technology implementation. Therefore, the FIS plays an important role in maintaining the integrity and sustainability of the financial system with regards to the implementation of technology.

The IT implementation in the financial institutions has helped improve the efficiency of operation as well as facilitate the innovation of the financial products. Especially for banks, IT implementation has been used to create competitive advantage for each individual bank service. The electronic banking product is one of the aspects considered by an individual or a corporation in deciding to become the bank's customer. The ease of transacting as offered by the implementation of IT has become one of the most important features in marketing a banking product. The availability of a highly sophisticated payment system also facilitates this development. Because of this, the banking industry is now becoming more dependent on the IT system. For this very reason, the IT risks have also been incorporated in the operational risk. Furthermore, the IT supervisory framework is designed to provide tools and guidance in conducting supervision on the IT-supported products, services, and operations in order to reduce and eliminate the IT risks within the financial institutions.

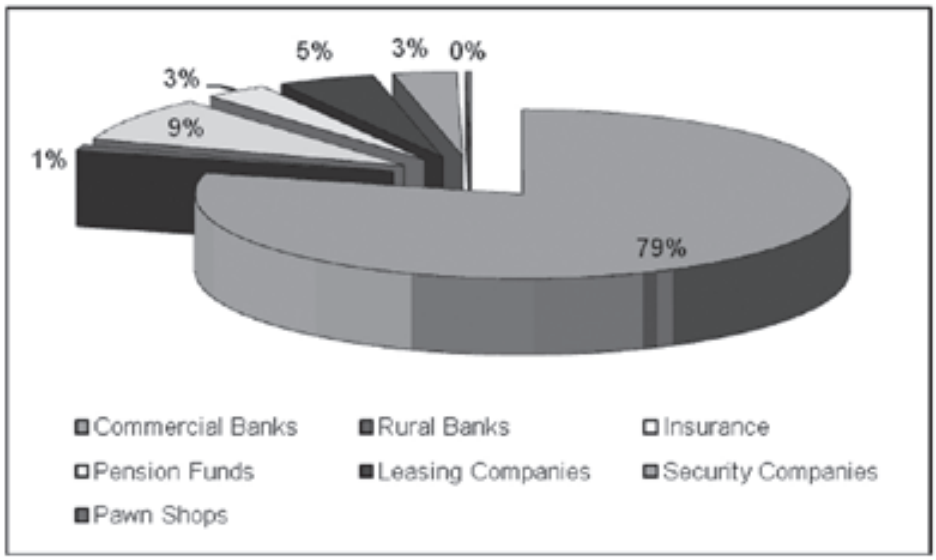
This paper aims to assess the state of technology-supported financial institutions in Indonesia, especially in terms of how technology can support the financial institution operation and boost the development of financial products. The paper is also part of the SEACEN research project set up to survey the issues and challenges of the IT supervisory impact on SEACEN financial institutions and to provide some suggestions for improvement within the region.

The rest of the paper will be arranged as follows. Section 2 will provide the overview of the Indonesian financial system. A more detailed survey on IT implementation in the financial system can be found in Section 3. Given the IT implementation, the impact will be described in Section 4. Section 5 outlines the prevailing IT supervisory framework and regulations. Section 6 will highlight the issues and challenges faced by the central banks and the financial institutions with regards to the risks posed by the IT implementation. Finally, the recommendations are presented in Section 7.

2. Overview of the Financial System

The Indonesian financial system is still segmented and dominated by the banking sector. The whole system comprises banks, which are divided into two groups consisting of commercial banks and rural banks[2], and non-bank financial institutions, which include insurance, pension funds, leasing companies, security companies, and pawn shops. The commercial banks' share in the total financial system is 79%, while 70% of the commercial banks' asset is held by 15 largest banks. Indonesia currently has 127 commercial banks with a total of 10,212 branch offices (as of July 2008). The commercial banks' total asset at the end of 2007 was Rp 1,986.50 trillion or equivalent to approximately US$ 210 billion. Figure 1 shows the share of each type of financial institutions in the Indonesian financial system.

Figure 1
Shares of Financial Institution Assets



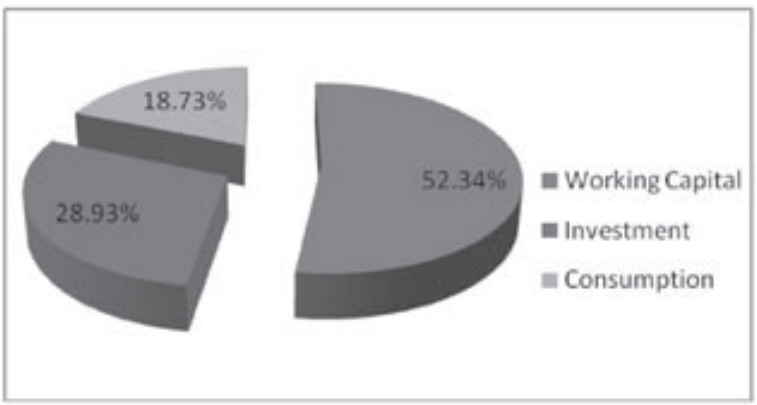
Even with the uncertainties in the global credit market, bank credit in Indonesia grew significantly in 2008. By July 2008, bank credit grew 32.3% y-o-y.[3] This is the highest y-o-y growth since the East Asian crisis. However, this is certainly a development that provides a mixed feeling, considering the problem of the global credit crunch and the fight over inflationary pressure. Bank Indonesia divides banking credit into three categories according to purpose: working capital,

2 Rural banks are translated from "*bank perkreditan rakyat*" or BPR, which mostly operate in the rural areas and are only allowed to provide saving and loan products.
3 Year-on-year; or growth as of July 2008 since July 2007.

investment and consumption. As of July 2008, credit for the productive sector (for working capital and investment) dominates the total credit. However, during 2008, the growth of credit for consumption has been the highest (19.8%), while the growth of credit for working capital the lowest (14.8%). The total credit has grown 15.8% y-t-d[4] since the beginning of 2008 (up to July). Figure 2 shows the shares of the three categories of credit in the total credit.

Figure 2

Shares of Banking Credit

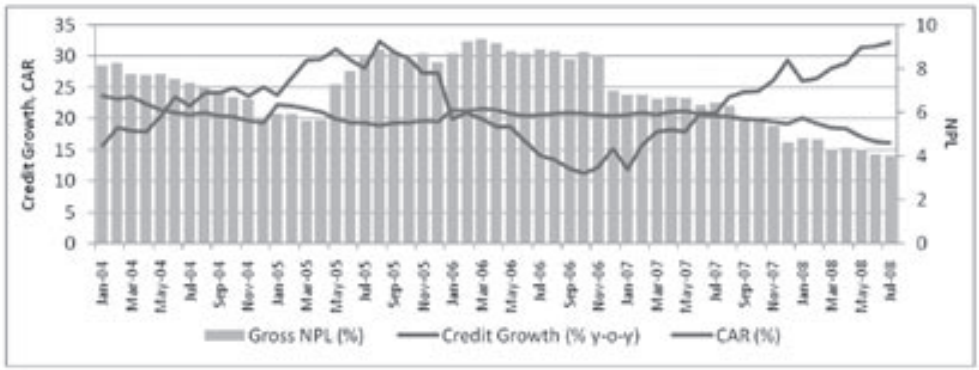


Credit for consumption, especially involving the use of credit cards, rides on IT implementation the most. The data of July 2008 shows that credit cards contributed to only 8% of the total growth of the consumption credit. In July 2008, credit involving the use of credit cards grew 31.9% y-o-y. The growth of credit by credit card usage is the lowest among the consumption credit.

Banking capital also has grown strongly following the momentum of recovery from the crisis of 1997-1998. As of July 2008, the commercial banks' CAR reached an average of 16.2%. However, this number is lower than the CAR in the beginning of the year (20.1%) and the CAR in July 2007 (20.7%). The expansion of credit in the first semester of 2008 may have been the reason for the declining CAR. Despite the aggressive credit expansion, the gross NPL has been declining. For the first time since the crisis, the gross NPL attained the level below 5% in December 2007, and the number has reached 4.0% in July 2008. Figure 3 illustrates the development of the three major indicators of the banking system during the period from 2004 to July 2008.

4 Year to date.

Figure 3
Credit Growth, CAR, NPL



The financial depth of the Indonesian financial system is very much determined by banking credit. Comparing Indonesia with the other four largest countries in ASEAN, using the indicator of claims on the private sector, the findings presented in Figure 4 show that the depth of the Indonesian financial system is among the lowest. Using. They also show the potential for Indonesia to increase the capacity of its financial sector to become the engine of economic growth.

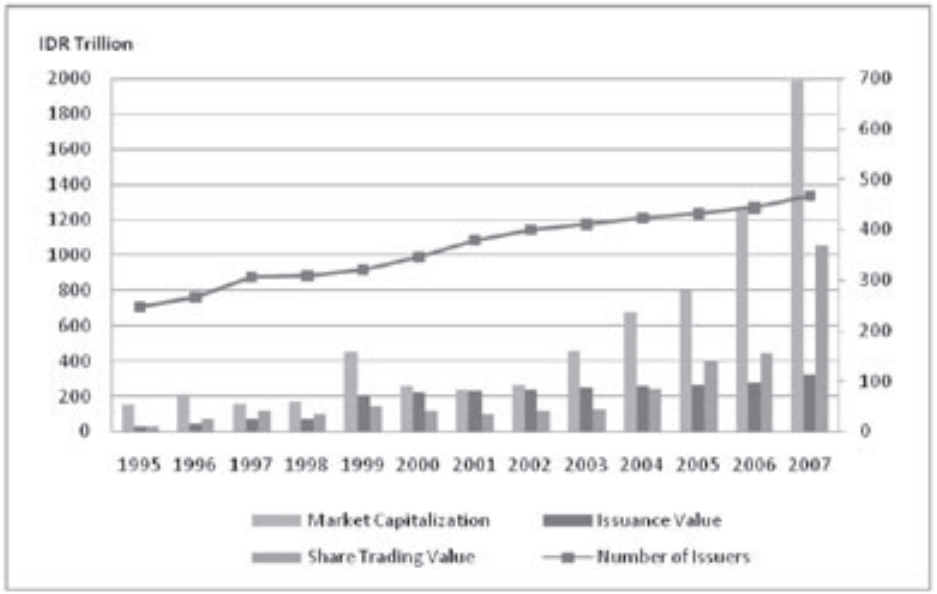
Figure 4
Credit to GDP Ratios of Five ASEAN Countries

Year	Credit to GDP Ratio (%)*				
	Malaysia	Singapore	Thailand	Indonesia	Philippines
2004	111.63	100.88	94.40	24.72	29.55
2005	110.59	95.20	93.07	25.54	25.86
2006	107.65	91.73	88.01	23.87	25.07
2007	105.13	95.72	84.34	25.12	23.84

*Source : Datastream. *Credit is proxied with Claims on Private Sector.*

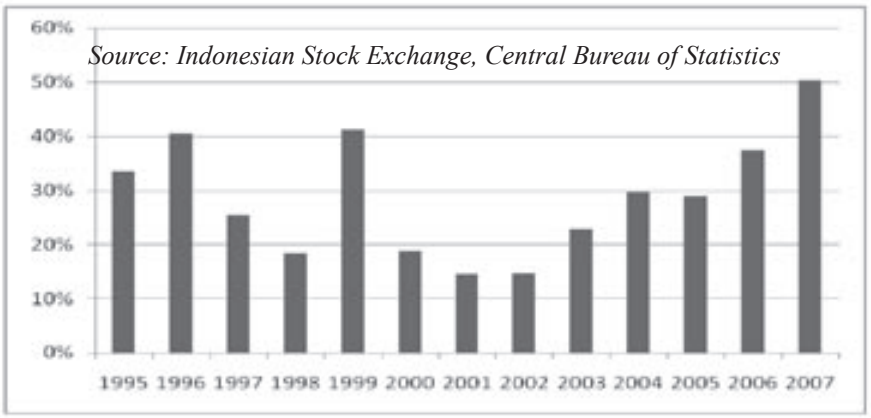
The development of the Indonesian capital market, especially fund pooling activities through the capital market, is very much influenced by the macroeconomic condition. This can be seen in the relatively slow growth during the period of 1997 to 1998 when the country was hit by the financial crisis. The number of issuers during that period only grew by 1% and value of issues increased by 7.1%. The bond market was even worse. There was virtually no new issue during this period.

Figure 5
Development of Issuers, Capitalisation, Trading Value, and Issuance Value 1995 – 2007 in Indonesian Stock Market



Source: BapepamLK

Figure 6
Ratio of Stock Market Capitalisation to GDP 1995 – 2007



Source: Indonesian Stock Exchange, Central Bureau of Statistics

Following stagnation during the period of the financial crisis in 1997-1998, the stock market rebounded in 1999 when corporations conducted restructuring exercises using the capital market. The value of issuance increased from Rp 75.9 trillion in 1998 to Rp 206.7 trillion in 1999, representing a jump of 172.2%. During the following period of 2000 to 2007, the value of issuance grew only at an annual rate of 6% whereas the number of issuers grew at an annual rate of 4.8%.

Market capitalisation during the period of 2000 to 2002 decreased following the unstable macroeconomic condition. However, the year 2003 saw an improvement in the macroeconomic environment and, as a result, the total value of market capitalisation grew to Rp 1,988.33 trillion as of March 2008. In 2007, the ratio of the market capitalisation to gross domestic product stood at 50.24%, which is a new record. However, the domestic stock market is not immune to the effect of the subprime mortgage crisis. The negative sentiments from the US contributed to the declining trend of the composite index. The index declined 33.26% from the end of 2007 to September 2008. The Figure 7 below shows the development of trading in the Indonesian Stock Exchange since the year 2000.

Figure 7
The Indonesia Stock Exchange (BEI) – Average Trading

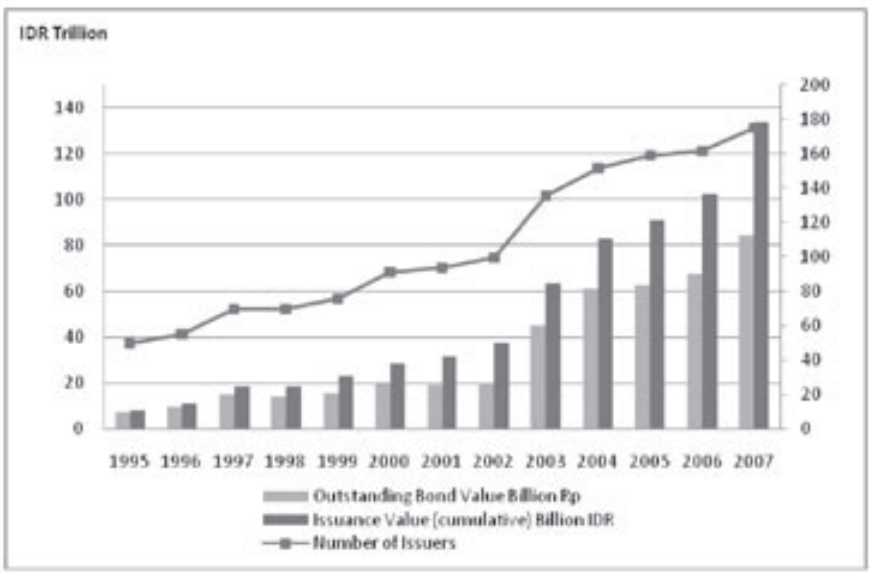
Indicator	*Composite Index*	*Average Value of Daily trading (billion Rp)*	*Average Volume of daily trading (million shares)*	*Average Frequency of Daily Trading (thousand)*
2000	416.32	513.70	562.89	19.22
2001	392.03	396.40	603.18	14.72
2002	424.94	492.90	698.80	12.62
2003	691.90	518.30	967.07	12.20
2004	1,000.23	1,024.90	1,708.58	15.45
2005	1,162.63	1,670.80	1,653.78	16.51
2006	1,805.52	1,841.80	1,805.52	19.85
2007	2,745.83	4,268.92	4,225.78	48.21
September 2008	1,832.51	4,041.95	3,317.52	60.52

Source : BappepamLK

The bond market suffered a great burden during the financial crisis in 1997-1998. There was no new issue of bonds in 1998. Meanwhile, the existing issuers faced difficulties in paying interest and even repaying the principal sum when the bonds reached maturity. However, the bond market rebounded in 1999 and attained top growth in 2003. During that year, the issuance value increased by 68.82% over the previous year and the number of issuers increased by 36% over the same period. The escalation continued until 2007. The number of issuers reached a total of 175 companies and the corporate bond issuance value reached a total of Rp 133.91 trillion. The significant progress of the bond market shows its increasing role as an alternative source of financing for the corporate sector.

The optimistic growth of corporate bonds has been well balanced with the development of Government Debt Securities (Surat Utang Negara or SUN). Beginning from September 25, 1998, the Indonesian Government issued some SUNs for Bank Indonesia, i.e. SUNs which were intended to finance the blanket guarantee program with respect to Bank Indonesia's Liquidity Support (Bantuan Likuiditas Bank Indonesia or BLBI) to prevent the collapse of the banking system during the financial crisis of 1997-1998. These securities cannot be traded. On May 28, 1999, the Indonesian Government started to use the capital market to pool public funds by issuing SUN to finance its banking restructuring program. These securities are tradable (government bonds). As of March 2008, the outstanding value of government bonds which can be traded reached Rp 541.70 trillion.

Figure 8
Development of Issuers, Outstanding Bond Value, and Corporate Bond Issuance Value 1995 – 2007



Like most central banks, Bank Indonesia is not the regulatory and supervisory authority for the non-bank financial institutions. The Supervisory Board of Stock Market and Non-Bank Financial Institutions (*Badan Pengawas Pasar Modal dan Lembaga Keuanga Non-Bank),* or BAPEPAMLK, is in charge of the non-bank financial institutions. Therefore, with regard to the survey of IT implementation, for the most part, we will be discussing the banking sector.

The widespread use of technology by the financial institutions also has the potential to spill over to the non-financial institutions. Companies are able to specialise in payment systems, such as credit cards, Internet payments and

transfer facility (e.g. GE and PayPal). These services will go undetected in the financial system as this type of companies is not regulated by the central bank. The proliferation of this type of companies will not only facilitate money laundering, but also it will create a distortion in the monetary statistics, creating difficulties in the prescription of monetary policy.

3. Survey of the IT Implementation

3.1 The Development of Technology Infrastructure

The latest means of communication are available in Indonesia. Telephone, fiber optic, and satellite communication are the usual means of telecommunication. Cell phone is becoming very popular in Indonesia, already reaching users in the low income bracket. By 2007, out of a population of more than 230 million, some 60 million people are using cell phones. Although the usage of cell phone technology is fast advancing, the same cannot be said of the usage of the Internet, which is lacking behind. The Internet is quite popular in the big cities since 1998, but it has yet to reach the smaller cities and the rural areas, except in the office compound of some big corporations. Although the Internet charge is still expensive, it is quite easy to obtain Internet access in the big cities. Some cafés provide hotspots, often offering free access. Users have a variety of ways of accessing the Internet, ranging from the narrowband to the broadband. They include dial up, cable connection, satellite, ISDN, DSL/ASDL and wireless connection. For corporations orspecializing, the use of domain names for email addresses and websites are quite common.

The national payment system is supporting non-cash payments in Indonesia. Although it mostly involves the banking sector, non-bank institutions are also linked to the system. These non-bank institutions support mostly credit/debit card payment and fund transfer/remittance services. Credit card networks include Visa, Master Card, JCB, and Diners Club. Debit card networks include Visa Electron (Visa International) and Maestro (MasterCard International). Some domestic banks operate their own debit card network, notably, the BCA Debit Card and Kartuku. The domestic remittance and fund transfer services involve the national postal company (PT. Pos Indonesia), and some other companies running businesses specializing in courier services, shops, travel agency, money changing, and also

with companies specializing in remittance services. The international fund transfer/ remittance networks include Western Union and Money Gram. Shared-ATM networks are also part of the national payment system. The international network for ATM includes Plus (Visa International) and Cirrus (MasterCard International). The domestic shared-ATM networks are ATM Bersama, LINK, Prima, Alto and Cakra.

The establishment of a sound payment system is part of the mission of Bank Indonesia. At the heart of the payment system is the Bank Indonesia Clearing System and the RTGS (real time gross settlement). Both are very important for the operation of the banking system. The Bank Indonesia Clearing System provides the following services: (1) debit funds transfers by means of electronically processed cheques, bilyet giro, debit notes; and (2) credit funds transfers processed electronically for small payments. The Bank Indonesia RTGS provides the following services: (1) high value interbank electronic funds transfers; (2) settlement of interbank money market, customer transfers, government transactions and monetary management; and (3) fund settlements for Bank Indonesia Certificates and Government Securities traded on the BI-Scripless Securities Settlement System (BI-SSSS).

In addition to the abovementioned systems, PT. KSEI (the Indonesian Central Depository) operates the clearing system for the capital market. This system, called the Central Depository and Book Entry Settlement System (C-BEST), provides for the fund settlements for securities transactions on the capital market. Four banks are involved in this system with whom the stock exchange members maintain settlement accounts.

The development of infrastructure in Indonesia is facilitating the progressive advancement of IT implementation by the financial institutions. In innovation, the IT-supported products will evolve utilising the latest technology from the more developed countries. Therefore, the opportunities for the Indonesian financial institutions for IT implementation and the launching of sophisticated IT-supported products may be boundless. The supervisory framework has to be ready for this.

Figure 9
Status of Installed IT Infrastructure

- *Are the following IT Infrastructure installed in the country?*

No.	Item	Yes/No
1	Communication Network	Yes
	Cable (Phone line)	Yes
	Satellite	Yes
	Fiber Optic	Yes
2	Use of Cellular Phone	Yes
	Is it relatively wide spread?	Yes
3	Use of Internet	Yes
	Is it relatively wide spread?	No
4	National Payment System	Yes
5	Operated by government agency / central bank	Yes
6	Operated by an independent or private company	Yes
7	Automated/Computerised Payment System	Yes
8	RTGS	Yes
9	National Securities Settlement System	Yes
	Operated by government agency / central bank	No
	Automated/Computerised Settlement System	Yes

3.2 The Presence of Technology-supported Financial Products and Services

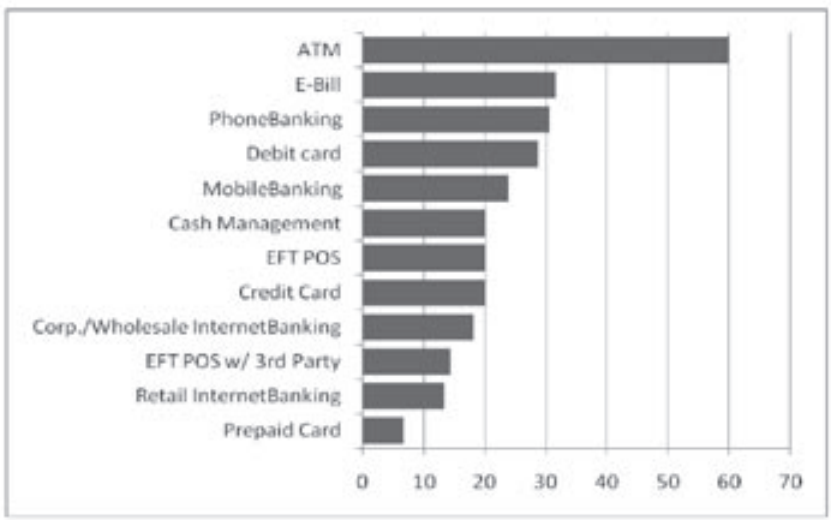
It is much easier to report the development of technology-supported financial products and services for banks than for non-bank financial institutions. Given the current development of banking products and services, it is difficult to imagine a full-fledged bank operating without some application of IT technology. In a Bank Indonesia survey conducted in 2006 to gather information on the latest development of IT in the banking sector, 105 banks out of the 130 banks surveyed responded. The survey provided some insights how most banks implemented IT in leveraging their business.

The implementation of electronic banking is definitely common in the Indonesian banking system. We can identify twelve different e-banking applications in the abovementioned survey. Automatic Teller Machine (ATM) is the most widely implemented application of e-banking (60%). There are only a few banks offering prepaid card products. E-bill ranks second as the most implemented feature of e-banking. The rest are shown in Figure 10. Payment by cheque is common for

business units (corporations). Payment by cheques is not a commonly acceptable practice for individuals, and this has contributed to the popularity of e-banking. Customers of banks seek practical ways of performing their transactions through e-banking. Although common in the big cities, credit cards have not yet reached the rural areas. Cash is still the most preferred means of payment settlement. For this reason, the ATM is widely popular in the banking sector. As of July 2008, Bank Indonesia registered 81 individual acquirers of ATM services. They are all commercial banks, with the exception of seven companies comprising four payment system companies, two rural banks and a pension fund.

When a point of payment is available, the debit card is the next most preferred payment mode. In some retail establishments, payment by credit card will attract an additional fee which is imposed as a percentage of the transaction amount. Nevertheless, credit cards have become a common means of payment in the larger cities. As of July 2008, Bank Indonesia registered 21 bank-issuers of credit cards, with a total of 10,678,891 of credit cardholders.

Figure 10
Percentage of Banks Implementing E-banking



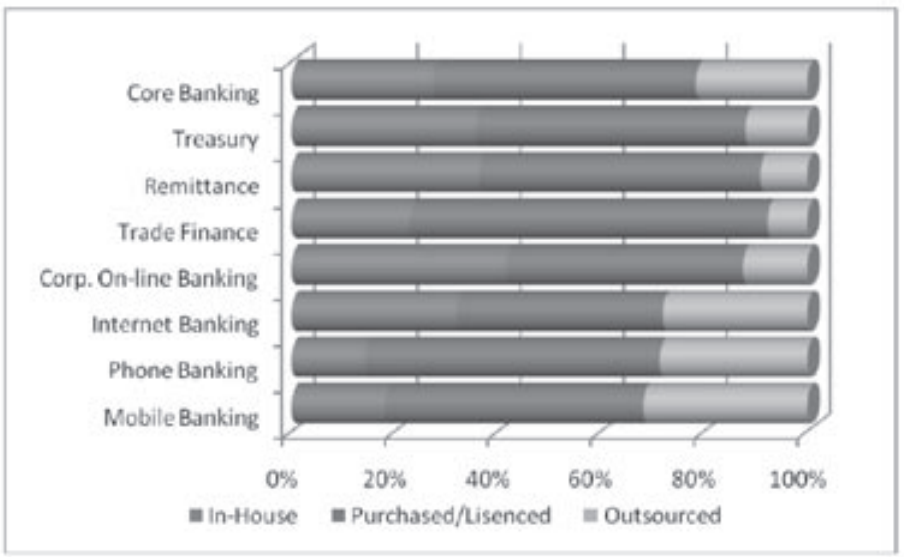
Source: Bank Indonesia Survey on IT Implementation by Banks of 2006

We also identify eight main components of IT implementation in the banking sector. They are: (1) Core Banking (comprising General Ledger, Third-party Fund, Loan and Customer Information File); (2) Treasury; (3) Remittance; (4) Trade Finance; (5) Corporate On-line Banking; (6) Internet Banking; (7) Mobile Banking; and (8) Phone Banking. Banks have different IT implementation policies for each of the components. Banks implement IT through one of these three ways: in-house,

purchased/licensed, and outsource. Figure 11 illustrates how IT is implemented in each component. The acquisition of a license to implement a system dedicated to operating a given component is quite popular. Among all the components, this type dominates the other choices of IT implementation (52%), and is especially popular for implementing Trade Finance (69%). In-house development comes in second on average (29%). For corporate on-line banking, banks are more balanced in choosing between in-house development and purchasing/licensing (42% and 46%). Security and data protection may explain for this. If not purchased/licensed, banks prefer outsourcing for mobile and phone banking services, whereas they are more balanced between in-house development and outsourcing for Internet banking.

The survey also reveals that only 50% of the banks implement continuous service procedure for e-banking services. This is quite a low percentage considering Indonesians have a high appetite for using e-banking services. Of the banks represented in this group, only about 10% implement criticality classification, 42% implement backup and recovery, and only 20% implement business continuity activation. This is an area that requires the attention of the Indonesian bank supervisors.

Figure 11
Types of IT Implementation



Source: Bank Indonesia Survey on IT Implementation by Banks of 2006

In the area of IT policy, the survey also reveals some facts. 82% of the banks surveyed have IT steering committees. 92% have risk management frameworks for IT implementation, although only 75% of this group conduct IT-risk mitigation evaluation. 71% apply standard operating procedure (SOP) for system development. All the responding banks have already implemented access restriction and division of authority for system and data. However, only 92% has IT security policy and 66% implement audit trail. With regard to IT auditing, in addition to being audited by Bank Indonesia, 73% conduct IT internal audit, 47% provide for IT external audit, and 21% conduct system/application internal audit.

The implementation of IT in the non-bank financial institutions is not less sophisticated. Although the author does not have survey information on IT implementation in the non-bank financial institutions (NBFI), the application of IT in these institutions has become part of the development of the financial market. In Indonesia, some financial institutions that are engaged in the stock markets implement e-trading. E-trading of stocks follows the regulations set by the Indonesian Stock Exchange (IDX). The supervisory framework of non-bank financial institutions follows the regulations set by the Capital Market and Non-Bank Financial Institutions Supervisory Agency (BAPEPAMLK). Phone and Internet access are the most common services provided for customers. Nevertheless, NBFIs are also exposed to all the risks that the banks are facing when they use IT for their operation. Therefore, the analysis of the supervisory impact should be the same.

Figure 12
IT–related Products

- *Are the following IT-related products implemented in the country?*

No.	Item	Yes/No
1	Credit Card	Yes
	National (only used in the country)	Yes
	International	Yes
2	Debit Card	Yes
	National (only used in the country)	Yes
	International	Yes
3	ATM	Yes
	Individual bank	Yes
	Nationally-shared ATM	Yes
	Internationally-shared ATM	Yes
4	Electronic Fund Transfer (EFT)	Yes
5	EFT at Point of Sale	Yes
	National (only within the country)	Yes
	International	Yes
6	Remittance Service	Yes
	Domestic companies	Yes
	International companies	Yes
7	Phone Banking	Yes
	Informational	Yes
	Transactional intra bank	Yes
	Transactional inter bank	Yes
8	Mobile/SMS Banking	Yes
	Informational	Yes
	Transactional intra bank	Yes
	Transactional inter bank	Yes
9	Internet Banking	Yes
	Informational	Yes
	Transactional intra bank	Yes
	Transactional inter bank	Yes
10	Pre-paid card	Yes

3.3 The Heterogeneity of the Technology Implemented in the Financial Institutions

The technology implemented in the Indonesian financial institutions definitely exhibits a high degree of variety. The abovementioned survey reveals that the budget for IT implementation in each bank ranged from 3% to 15% of the total non-interest operational budget, with 75% to 90% realisation of the budget. The fact that the Indonesian banks are heterogeneous in terms of their business model and size drive the heterogeneity of the technology that is implemented to support the banking products and services. This poses difficulties in standardising the IT practices of the banks. Banks with less sophisticated technology may consider maintaining a low budget for their technology development and operation. This means that they may find it too costly for them to implement all the IT supervisory best practices, such as disaster recovery plan and IT audit.

In terms of supervision, the heterogeneity of the IT systems increases the complexity of the standard operating procedure for IT supervision. Banks may have different levels of risks in different areas of IT implementation. For example, each of the three ways of implementing IT, as mentioned earlier, poses a different level of risk and supervisory techniques. The IT specialists are also confronted by a variety of software and hardware that are being used by banks in their IT implementation that requires the mastering of different skill sets. The challenge for conducting IT supervision in a such a heterogeneous environment is greater than in a homogeneous environment.

To add to the complexity, sophisticated IT implementation requires more qualified IT supervisors. In practice, professional IT auditors may not work for the central bank or financial institution authority. With the number of banks that need to be supervised, it may be too costly for a central bank or a financial institution authority to employ qualified IT specialists and auditors. The alternative is also expensive: outsourcing the IT auditing function to an independent IT auditing company. Therefore, in the IT supervisory framework, Bank Indonesia requires banks to have adequate IT auditing, and submit the audit report to Bank Indonesia. This is deemed to be sufficient until further human resources development can be done to upgrade the IT skills of bank supervisors.

Figure 13
Status of IT-related Applications in addition to IT-related Products

- *Regarding IT-related Applications in addition to IT-related products, are the following applications implemented with IT?*

No.	Item	Yes/No
1	Core Banking: General Ledger, Third Party Fund, Loan, and Consumer Information File	Yes
2	Treasury	Yes
3	Remittance	Yes
4	Trade Finance	Yes
5	Corporate Online Service	Yes

4. Impact of IT Implementation on Financial Institutions

IT implementation opens up new horizons for the launching of innovative products and services. However, the deployment of IT technology is not without hazards. The most efficient banks[5] in Indonesia implement highly sophisticated IT systems in order to gain a competitive edge. Customers will be attracted to banks that can provide them with the widest range of products and services suitable for their needs. Therefore, the banks that are financially strong will attempt to implement the latest technology to attract customers. While IT systems can eliminate human errors, they do not come without risks. The reliance on IT to drive banking operation increases the factors that bankers need to consider in controlling the operational risks.

4.1 Assessment of the Types of Risk in Regard to the Technology-supported Financial Products and Technology-supported Financial Institution Operation.

The dual role of technology pose different areas of risk[6] for the financial institutions. In general, the second role of technology poses more operational risk than strategic risk when performed inadequately. It is the other way around for the first role. However, when managed improperly, both roles pose reputational, legal and compliant risk.

---

5 The efficiency of the banks is measured with the ratio of operational cost to operational revenue.
6 Recall that technology has dual role in the development of finance: as engine of development of financial products and as engine of the financial institution operation.

Based on the IT systems implemented by banks, Bank Indonesia recognises five types of risks related to IT implementation. They are:

i. *Operational risk*: This risk is attached to every product and service provided by the banks. This risk emerges from inadequate or improper design, implementation, system maintenance, security method, testing, internal audit standard, and outsourcing;

ii. *Compliant risk*: This risk rises when the IT implementation does not comply with the prevailing regulations, such as when the confidentiality of the customers' information is violated or when the mechanism of the transaction violates the prevailing financial transaction regulation. This risk may damage the reputation and image of the banks;

iii. *Legal risk*: Banks face legal risk posed by legal suit, absence of supporting service level agreement, or weakness in the service agreement;

iv. *Reputational risk*: Negative rumours can emerge because of a failure in the IT system that supports the bank's products or a failure to provide services during downtime. The rumours may undermine the bank's ability to maintain the customer's loyalty and successful products and services marketing;

v. *Strategic risk*: This risk emerges from the bank's decision-making process in implementing the IT. The IT design, the IT-supported product design, the hardware, software and human resources (brain-ware) or the choices of IT infrastructure may not be suitable for the strategic objectives of the bank.

In general, Bank Indonesia does not impose a standardised method to measure IT risk. Nevertheless, Bank Indonesia uses IT guideline[7] as a reference. The IT guideline comprises ten chapters that bank supervisors have to pay attention to when conducting on-site examination. Banks also have different ways of measuring operational risks, in which IT risk is included. The survey mentioned in Section 2 reveals that about 50% of the banks responding to the survey have included IT risk in their risk management framework.

4.2 Risks and Impact of the Use of IT in Financial Products and Financial Institution Operation in Relation to the Supervisory Practices

Specifically, in regard to the implementation of IT in the banking and payment system of Indonesia, the risks may emerge from these sources:

7 Guideline for Risk Management in the Use of IT by Commercial Banks (Bank Indonesia Circular Letter No. 9/30/DPNP dated December 12, 2007)

i. **Substandard IT implementation**
Bank Indonesia emphasizes concern in this issue. Banks that implement substandard IT systems are at risk of IT failure. When these banks are dependent on the IT systems, the IT failures will disrupt their operation. Substandard IT implementation poses operational and reputational risk.

ii. **Cyber crime** (such as phishing, personal identity theft, etc.)
This risk of cyber crime may have yet to be mitigated by sufficient law enforcement. Indonesia recently enacted a cyber law in Act No. 11/2008 dated April 21, 2008. The government needs to foster increased legal awareness in the cyber society and raise the technical skill of the law enforcement officers in detecting legal violations. Cyber crime may not be a major threat as yet. Nonetheless, the implementation of the law anticipates and caters for the growing use of the Internet for transactions. The need to increase awareness of the importance of complying with the cyber law in Indonesia remains an issue of concern, if Indonesia is to keep up with the international standard of the cyber community. Even before the enforcement of cyber law, Internet banking transactions have become common place in Indonesia. Banks providing for this type of service are called to take sophisticated security measures to safeguard their IT systems.

iii. **Payment system companies**
These companies offer payment services (remittance, non-bank credit cards) that are not supervised by the financial institution supervisors and they have less restriction on capital requirements. They may become an avenue for money laundering.

iv. **Social engineering**
This may have a high probability of success in Indonesia given the huge appetite of customers in seeking more convenient ways to make payments, fund transfers and remittances. Those who are not aware of the risk in social engineering may risk becoming victims. For example, people may not be aware that giving other people their personal information may expose them to the possibility of identity theft.

v. **Customer's ignorance of the terms and conditions of the products**
This may be another source of IT risk. When customers ignore the fine print of the agreement, they are often unaware of the terms and conditions for them to gain the most out of their bank accounts (e.g. avoiding fees, making sure that the bank is providing the level of service as promised). Bank Indonesia has required banks to provide clear information for their products as well as provide technical support for customers of IT-supported products.

Figure 14
Types of Risks

- *IT Risks*
  As to the impact of the level of IT Implementation in the country, what are the risks that need to be addressed and controlled in the financial system?

No.	Item	Yes/No
1	Operation Risk	Yes
2	Liquidity Risk	Yes
3	Credit Risk	Yes
4	Strategic Risk	Yes
5	Reputation Risk	Yes
6	Legal Risk	Yes
7	Compliance Risk	Yes

4.3 Strengths and Weaknesses of the Supervisory Procedure in Indonesia

Bank Indonesia has placed emphasis on the standard of IT implementation in the banking system to ensure that banks practise good IT governance. The IT supervisory framework started with the offsite supervision of banks for their IT implementation. Banks are required to do standardised reporting in regard to their IT implementation by answering the questionnaire prescribed by Bank Indonesia. Today, Bank Indonesia practices different levels of treatment for banks in terms of IT supervision. Bank Indonesia conducts targetted visits for IT audits for banks operating highly sophisticated IT systems. Some of the bank supervisors are IT specialists who are specialised in the supervision of the implementation of risk management in the IT system.

The continuing drive to incorporate IT risk within the overall risk management framework of the banking system has become one of the strengths of the IT supervisory framework in Indonesia. Although the IT supervision has been integrated with the overall supervisory framework before the East Asian crisis in 1997, Bank Indonesia established the first regulation for its IT supervisory framework with the promulgation of the Bank Indonesia Regulation (PBI) No. 9/15/PBI/2007 dated November 30, 2007, and the Bank Indonesia Circular Letter (SE BI) No. 9/30/DPNP/2007 regarding the Application of Risk Management in IT Implementation by Commercial Banks. This regulation will be explained further in Section 5. The regulation has helped increase the awareness of a need for controlling IT risks within the banking system. To be competent in carrying out IT risk assessment, bank supervisors are required to master the latest development of the IT architecture of the bank, the standard operating procedure, the structure of the IT management, and the IT risk management. Therefore, a period of 12 (twelve) months are given to the banks to comply with the requirements of the current IT supervisory framework.

Given the established regulation, Bank Indonesia still have some homework to do in order to for the organisation to move forward. Its pool of IT specialists has to be further enlarged and their competencies improved. As in the other countries, the central bank is faced with the challenge of determining how qualified an IT specialist should be, and what is the appropriate frequency in conducting IT supervision. The heterogeneity of the IT systems in the banking sector adds to the complexity in determining the standard IT audit practice required for each bank.

5. Prevailing IT Supervisory Framework and Regulations

The use of IT in Indonesia is stipulated in the Act No. 11 of 2008, dated April 21, 2008, regarding Electronic Information and Transaction. This Act acknowledges that the fast development and advancement of IT have changed the way people conduct their affairs in different fields. This has, in fact, led to the enactment of new legislation. The above Act upholds the importance of developing the use of IT for trade and economic development as a means of improving social welfare and of contributing towards the achievement of national unity. This Act also enunciates provisions for the safe and proper implementation of IT, based on the religious, social and cultural values of Indonesia.

Bank Indonesia has provided the legal framework for IT implementation in the banking industry even before the establishment of the abovementioned Act. The latest regulations are Bank Indonesia Regulation (PBI) No. 9/15/PBI/2007, dated November 30, 2007, and Bank Indonesia Circular Letter (SE BI) No. 9/30/DPNP/2007, dated December 12, 2008, regarding Risk Management in the Use of IT by Commercial Banks. This regulation, henceforth referred as BI regulation

on IT risk management, has also incorporated the implementation of the risk-based management in accordance with the Basel II supervisory framework. Bank Indonesia then established the IT supervisory framework to ensure the banks are compliant to the PBI.

5.1 Principles

The IT supervisory framework is formulated by Bank Indonesia based on the following premises:

i. IT development allows banks to increase the efficiency of their operations and the quality of their customer/client service;
ii. The use of IT in the operational activities of banks can also increase the risk faced by banks;
iii. Banks need to implement risk management effectively with the increase of risk caused by IT implementation;
iv. IT system is a valuable asset for bank so that the IT department should not be the only unit responsible for the management of the IT system; and
v. Adequate IT system is important for the implementation of the Basel II framework.

The IT supervisory framework is established to achieve with these objectives:

i. Provide bank customers protection in regard to the use of IT-supported products;
ii. Inclusion of IT risks to ensure the development of effective risk-based management framework of banks. This becomes important since IT implementation is also a source of revenue (fee-based income); and
iii. Ensure the compliance of the IT implementation to the prevailing acts and regulations, especially in respect of Bank Indonesia enactments, anti-money laundering, and know your customer.

5.2 Regulatory Framework and Regulations

In essence, the abovementioned PBI addresses the following items:

i. The minimum requirements for IT implementation in banks are:
   1) Active supervision by the Board of Commissioners and Directors;
   2) Adequate IT Operational Policy and Procedure;

3) Adequate process in identifying, measuring, monitoring, and controlling IT risks; and
4) Internal control system for IT implementation.

ii. According to the BI regulation on IT risk management, banks are required to implement risk management consisting of the identification, measurement, monitoring, and control of the risks associated with the use of IT. In the development of risk-based management system for IT implementation, attention should be paid to:
1) The function of the IT Steering Committee in giving recommendation to the Board of Directors in regard to the strategic planning for IT development and implementation in order to ensure the IT implementation plan is aligned to the overall business plan of the bank;
2) The establishment of IT policy and standard operating procedures that contain at least the aspects of management, development and purchasing, IT operations, communication network, information security, and outsourcing;
3) The existence of Business Continuity Plan and Disaster Recovery Plan that has been tested at least annually;
4) The protection of information to ensure confidentiality, integrity, and availability of the information. This includes the aspects of technology, human resources and processes in the use of IT, and covers bank asset management related to information, human resources policy, physical security, access security, operational security, and other aspects of IT implementation.
5) The conduct of periodical IT internal or external audit. In the case of limitation of the ability of internal auditors, banks are allowed to hire external auditors.

iii. In the case of outsourcing:
1) Banks can implement an in-house system and/or outsource the IT services to an IT vendor provided they comply with the following requirements:
a) Bank is still responsible for the application of the risk-based management;
b) The IT vendor can guarantee the security of the information, including the privacy of the banking and customer/client's data;
c) The IT vendor is providing access to the information for internal auditors, external auditors and Bank Indonesia supervisors;
d) The IT vendor is willing to accept early termination of the service contract if is later found that the service contract is causing difficulties in the conduct of banking supervision by Bank Indonesia.

2) Banks should permit the internal auditors, external auditors, and auditors from Bank Indonesia to have access to data and information, whenever needed. This should be done in a timely manner for current and past data.
3) Outsourced Data Center (DC) and Disaster Recovery Center (DRC) are required to be located in Indonesia. If they are not located in Indonesia, Bank Indonesia's pre-approval is necessary, and the banks have to fulfill the abovementioned requirements for outsourcing as well as additional requirements.
4) The outsourcing of the process for IT-supported transactions can only be carried out with pre-approval from Bank Indonesia. The bank is required to comply with the abovementioned outsourcing requirements as well as meet additional requirements:
    a) The activities outsourced are not inherent banking function activities;
    b) The supporting documents of the transactions done in Indonesia have to be maintained in the bank office located in Indonesia;
    c) The bank's business plan indicates that the bank is making effort to expand its role in the development of Indonesia's economy.

iv. Electronic Banking (e-banking)

Banks launching an e-banking product entailing financial transactions are required to include the implementation plan in the bank's business plan, and the documents are to be submitted to Bank Indonesia two months before the product launch. The submission has to be accompanied by a product assessment to be performed by an independent reviewer in regard to the product characteristics and the adequacy of the IT security. Banks are also required to furnish a product educational programme for educating their customers on the e-banking product and its security features.

Figure 15
Status of IT Supervisory Framework

- *Regarding IT supervisory framework,*

No.	Item	Yes/No
1	Is IT Implementation reported regularly?	Yes
2	Is IT audit conducted?	Yes
	By bank/IT supervisors from supervisory authority	Yes
	Off-site	Yes
	On-site	Yes
	By internal or external (third party) auditors (on-site)	Yes
	Special IT audit/examination outside regular examination (on-site)	Yes
3	Does the formal framework exist?	Yes
4	If yes, is it stipulated in a regulation?	Yes
5	Is there minimum requirement in IT Implementation?	Yes
6	Are the following items implemented: Active supervision by Top Management (IT Steering Committee)	Yes
	IT Policy and Standard Operating Procedure	Yes
	IT risk is included in the risk-based management	Yes
	System development life cycle	Yes
	All layers of IT system	Yes
	Internal control system for IT Implementation	Yes
	Business Continuity Plan and Disaster Recovery Plan	Yes
	Periodical IT audit (internal/external)	Yes
7	Because it involves supervision procedure, is IT outsourcing especially regulated?	Yes
8	Because it involves consumer protection, is e-banking products especially regulated?	Yes
9	Are any IT-related laws (cyber law, e-commerce, m-commerce, digital signature) installed?	Yes

5.3 References / Orientation for the Prevailing Supervisory Framework

Bank Indonesia designed the regulatory and supervisory framework for IT implementation by referring to the regulations and frameworks applied in various countries with adoption of the best practices in IT implementation, subject to adjustments in Indonesia's banking conditions. COBIT, ISO standard on IT security and IT management, ITIL certification, FFIEC (of the U.S. Federal Reserve) and IT supervisory frameworks implemented in Hong Kong, Malaysia and Singapore are the main sources referred to during the formulation.

5.4 IT Supervision and Audit Practices

The IT supervision and audit practices are done by profiling the IT risk management of the bank. The objectives of the process are:

i. to measure the risk exposure inherent in the bank within the framework of the bank's risk-based management;
ii. to support bank supervisors in recognising the weaknesses in the IT implementation and the risk level faced by the bank;
iii. to provide an early warning system regarding the IT conditions that may require special attention from the bank supervisors; and
iv. to determine the coverage and frequency of IT audit.

The profiling process is done internally (by the bank supervisors) and integrated between off-site and on-site supervision. The informational sources for the profiling exercise consists of the IT implementation report and data supplied by the banks, supervisory report by the bank supervision team, working documents and examination report that includes general control, application control and technical control.

IT supervisory framework recognises the three inherent risks in IT practices: (1) operational risk, which includes system failures, human errors and/or frauds, and strategic failures; (2) legal risk, which includes outsourcing and IT service-sharing contracts and claims on violation of copyrights; and (3) reputational risk, which includes negative publicity associated with customers' claims and system failures. The risk is measured by the weighted average of the scores of the inherent risks.

Figure 16
Status of IT Audit

- *Regarding on-site IT Audit,*

No.	Item	Yes/No
1	Is it conducted regularly?	Yes
2	If not regularly, is it conducted case by case?	
3	If regularly, objects of audit:	
	Organization and Management	Yes
	System development process	Yes
	Operation	Yes
	Software and Application, including E-banking	Yes
	Security (authentication, authorization and protection – including audit trails, encryption)	Yes
	BCP/DRP	Yes
	Communication Network	Yes
	Outsourcing process	Yes
	Internal Auditing	Yes

5.5 IT-specialised Supervisors/Auditors

Bank Indonesia currently employs 20 IT specialists to supervise 128 banks grouped under three banking supervision directorates (Directorate of Bank Supervision I, II and III). This is not a good ratio. Therefore, Bank Indonesia is embarking on a training programme for all banks supervisors to learn the basic skills of IT auditing and providing opportunities for them to become IT specialists. The general training is divided into two different types of bank supervisors: all bank supervisors and IT specialists. Bank supervisors will receive "Basic IT Auditing I", which includes basic IT auditing, general IT control, application control, core banking systems, credit card, treasury, trade finance, payment system and electronic delivery system (e.g. ATM, Internet banking, etc.). IT specialists will receive more advanced training, ranging from "Basic IT Auditing II" to "Computer Forensics," to better equip them for conducting IT audit. Training is given in specific areas, such as IT for leaders, specific application, operating systems, database, and certification for IT auditors. Bank Indonesia has recently conducted two preparatory CISA (Certified Information System Auditor) training sessions catering not only for IT auditors and IT staff in Bank Indonesia, but also for other bank supervisors in Bank Indonesia's Head Office as well as branch offices. 30 people have participated in each session.

To ensure Bank Indonesia can compete with corporations in the hiring and retention of highly skilled resources in IT supervision and professionals specialising in IT auditing, Bank Indonesia plans to establish a career path for bank supervisors who possess high IT skills and the passion to become IT auditors. A task force is already assigned to chart this career path in conjunction with the Human Resources Directorates and the three banking supervision directorates. The 20 IT specialists are currently distributed among these three directorates. The career path will offer IT auditors a competitive compensation package relative to the other positions in the core functions of Bank Indonesia and the package of IT auditors working for IT companies.

5.6 Coordination among Financial Institution Authorities

Coordination among the financial institution authorities is an important factor in safeguarding the financial system stability. IT supervision is a part of the financial institutions' supervisory framework. In designing the blue print of the Indonesian Financial System Architecture, the financial institution authorities - Bank Indonesia, BAPEPAMLK, and LPS (Deposit Insurance Company) - have emphasized the importance of the supervisory framework as part of the foundations / pillars making a sound and stable financial system. The financial institution authorities are also designing the financial safety net (FSN) mechanism. The FSN mechanism will be activated when crisis occurs at the institution and market levels.

6. Issues and Challenges

6.1 Issues

- The perception and awareness of the importance of including IT risk in the risk-based management framework. The supervisory framework may already include IT risk as part of the overall risks faced by banks. Because IT risk is something rather new, some supervisors may neglect to pay attention to IT risks when conducting IT supervision. IT audit may be a difficult task, but it is an important one.

- Standard qualification of IT auditors for financial institutions. In regard to the bank supervisors employed by the central bank, how skillful should an IT auditor be? Hiring a skillful IT specialist from the market may be expensive. Although possible, developing and tooling bank supervisors to become skillful IT specialists is a long haul proposition. When the bank succeeds in producing skillful IT specialists, it will encounter the risk of losing the IT specialist to better pay from the market. Do central banks need to impose binding working contracts for potential skillful IT specialists before training them?

6.2 Challenges

- IT supervisors have the responsibility of making sure that IT governance is practiced by all the banking institutions. The challenges include:

  a. Understanding IT process;
  b. Understanding IT-supported product mechanism;
  c. Assessing the IT risk:
     i. Periodic assessment: determining the frequency that is appropriate for each institution;
     ii. Coverage of all layers of the IT system;
     iii. Enforcing the requirement for financial institutions to establish a fund to cover customers on IT frauds, thefts and failures.

- How to establish an IT supervisory framework in a heterogeneous environment. Enforcing a uniform standard across the board will be unfair. Banks with less sophisticated IT systems will to incur a large investment in order to comply with the standard. In the meantime, the standard may not be sufficient for banks with highly sophisticated IT systems.

- Discouraging "social engineering" by establishing market discipline among customers: "protect your password/PIN," "know the risk and security features," "use your e-banking and e-trading features at your own risk." This effort is actually in line with the government effort to increase awareness of the cyber society about IT risks.

7. Recommendations

The implementation of IT depends for its success on the commitment of the top management of the financial institutions. The IT supervisory framework depends for its operational effectiveness on the total commitment of the financial institutions and the authorities. On the part of the central bank, the commitment from the bank supervisors at all levels is important. Considering the existing IT proficiency level of the bank supervisors, this is easier said than done. Increasing IT risk awareness in the supervision of financial institutions is a matter of concern to the top management of the central bank. Indonesia has yet to face a financial crash caused by IT system failure. However, we should not wait for it to happen before we include the IT risk in the supervisory framework.

In addition to the inclusion of IT audits in the supervisory practices, Bank Indonesia has laid down the minimum requirements for IT Implementation, as described earlier. These requirements need to be evaluated periodically in the light of the potential risks indicated from the findings of the IT audits. The supervisory framework needs to follow the development of IT. We are fortunate to be able to learn from the experience of the developed countries in establishing the IT supervisory framework. The framework should take into account the state of IT system development as well as the nature and the trend of IT practices in the country.

The next issue of concern should be the proficiency requirements of IT supervisors and auditors. Since the concern over IT risks intensified only lately, Bank Indonesia has yet to fill the need to have qualified IT auditors, specialists in IT auditing, to complement the financial auditing by the bank supervisors. It is to be noted that it is not easy to find a person that can perform financial and IT auditing at a high level both at the same time. Bank Indonesia has started organising training programmes to equip bank supervisors in the basic skills of IT auditing, while providing training for bank supervisors who desire to specialise as IT auditors. Going by a different approach, Bank Indonesia also recruited some IT auditors from different entry levels in order to do special investigation of the IT system of a bank when needed. To overcome the shortage of IT specialists in the banking supervision units, Bank Indonesia may require banks – especially those with highly sophisticated IT systems - to have outsourced IT auditors report directly to Bank Indonesia.

In order to bring SEACEN countries to a level playing field in terms of IT implementation, SEACEN should provide a forum where central banks can share their experience and the lessons learned in IT supervision. The SEACEN forum may even recommend measures for member countries to take to help them overcome some of the difficulties of IT supervision, or measures to assist them in establishing the IT supervisory framework. This exchange of country experience may be insightful in helping SEACEN member countries avoid the problems and difficulties encountered by other countries in the region. The heterogeneity of the IT systems in Indonesia sometimes requires the bank supervision units to conduct IT auditing with different intensities for different banks. This is the experience of Indonesia that may be shared with other countries in the region.

References

Bank Indonesia, "Regulation of the Application of Risk Management in Information Technology Implementation by Commercial Banks," Directorate of Banking Research and Regulation, Bank Indonesia, 2007.

Bank Indonesia, "Supervisory Guidance for the Application of Risk Management in Information Technology Implementation by Commercial Banks," Directorate of Banking Research and Regulation, Bank Indonesia, 2007.

Barouski and Beutel, "Supervisory Impact of Technology on South East Asian Banking," The SEACEN Center, Kuala Lumpur, Malaysia, May 1999.

Basel Committee on Banking Supervision, "Management and Supervision of Cross-Border Electronic Banking Activities", Bank for International Settlements, July 2003.

Basel Committee on Banking Supervision, "Risk Management Principles for Electronic Banking", Bank for International Settlements, July 2003.

GTAG (Global Technology Audit Guide), "Management of IT Auditing," The Institute of Internal Auditors, March 2006.

IMF & World Bank, "Financial Sector Assessment: A Handbook," International Monetary Fund and the World Bank, 2005.

Katz and Shapiro, "Systems Competition and Network Effects," *The Journal of Economics Perspective,* Vol. 8, No. 2, (Spring 1994), pp. 93-115.

Shapiro & Varian, "Information Rules: A Strategic Guide to the Network Economy," Harvard Business School Press, November 1998.

Varian, "The Economics of Information Technology," Cambridge University Press, January 31, 2005.

CHAPTER 5

THE SUPERVISORY IMPACT OF TECHNOLOGY ON SEACEN FINANCIAL INSTITUTIONS: ISSUES AND CHALLENGES IN MONGOLIA[1]

by Tsolmon Baasanjav[2]

1. Introduction

"Technological innovation affects not just banking, financial services, and regulatory policy, but also the direction of the economy and its capacity for continued growth." (Ferguson, 2000)[3]

We all know how tremendously fast and how extremely well the developments and improvement in information technology advance around the world. In every country, the developments in information technology and infrastructure facilitate the smooth running of businesses, marketing of business products and services, and the generation of income and capital. For most emerging markets, their advancement in the adoption of information technology has contributed to their integration with the global economy. Although the GDP of Mongolia is growing, the relatively low GDP per capita (amounting to US$1,300 as of the end of 2007), does not explain the relatively high ratio of cell-phone ownership to the population (amounting to 49.1%), if compared to other countries with a similar level of development.

With the development of the banking and financial system in Mongolia and the introduction of more sophisticated financial products, information systems play a crucial function in the management of the financial institutions. To compete in the marketplace, the financial institutions introduce information technology/ infrastructure-based products to satisfy customer needs and improve their internal operational efficiency. Out of the 16 banks operating in Mongolia, ten have issued bank cards to facilitate the payment and transaction needs of their customers.

---

1 In Mongolia, the Bank of Mongolia (central bank) is the authority for the regulation of banking institutions only. Therefore, this paper will focus on the banking sector only. Although most of the materials included to this paper are quoted from the Bank of Mongolia's supervisory framework, the views and opinions are solely those of the author only.

2 Author is Supervisor, Policy and Regulation Division, Supervision Department, Bank of Mongolia. The author appreciates the helpful suggestions and comments of the Research Director - Dr. John Junggun Oh (Director of Research, The SEACEN Centre), Project leader - Dr.Cicilia A.Harun (Researcher at the Financial System Stability Bureau, Directorate of Banking Research and Regulation, Bank of Indonesia), Workshop Discussant – Dr. Haibin Zhu (BIS), and all my colleagues – the research team members and participants of the workshop on SEACEN Research Project "The Supervisory Impact of Technology on SEACEN Financial Institutions: Issues and Challenges".

3 Quoted by Dr. Haibin Zhu, during the SEACEN Workshop on "The Supervisory Impact of Technology on SEACEN Financial Institutions: Issues and Challenges".

It is undisputable that the implementation of IT innovations in the financial sector confers benefits to all the financial institutions, their customers and the regulatory bodies. For the financial institutions, the major benefits they enjoy, as highlighted by other research works, include IT developments leading to a reduction in operation cost; improvement in efficiency; attraction of new customers by enhancing the convenience, speed and, thus, the value of the existing products/services; abolishment of the geographical restrictions; development and implementation of sophisticated risk- and information-management systems; and greater competition and better value for money. For the consumers, the gains are faster and more convenient service, greater competition and better choices, with all these translated into better value for money. Similarly, for the regulatory bodies, IT developments have the potential in facilitating the communication of faster and better quality information and contributing to easier monitoring. Researchers point out that, based on purpose and degree of sophistication, the adoption of IT in the banking sector, can be categorised in two general stages: first, when information technology is used as an engine of operation, and second, when information technology is used as an engine of financial development.

During the first stage, banks utilise IT as an engine to drive their operations, i.e. IT is applied for data processing (introduction of automated bookkeeping machines and development of management information systems). It is subsequently deployed to create new channels for the delivery of the existing services (introduction of electronic payment systems, e-banking services like Internet banking, phone banking, and ATM, and e-financial products, like online brokerage). Countries, which are advanced in IT and banking sector development, deploy IT as an engine of financial development, applying IT in the banking sector for the purpose of creating of completely new and innovative products and services, like e-money and other financial innovations in value creation, valuation and risk management.

Needless to mention, risks manifest with the inappropriate maintenance and operation of information systems. Inadequate management of information systems risks may hinder not only the financial position of the financial institutions, but also the business of their customers, thus impacting the stability of the whole financial system and economy of Mongolia. The formulation of a proper regulatory and supervisory framework for IT-risk management in the commercial banking sector is one of the major challenges facing bank supervisors in the Bank of Mongolia.

Accordingly, it is the purpose of this paper to survey the status of IT implementation by commercial banks in Mongolia and to evaluate the appropriateness of the regulatory framework to be implemented by the Bank of Mongolia in regard to its role of ensuring financial system stability as well as its role in the monitoring and supervision of commercial banks. Following

this introduction, an overview of the financial system is outlined in Section 2. In Section 3, the findings of the survey of the implementation of information technology in Mongolia are presented. In Sections 4 and 5, the supervisory impact of IT implementation and the status of the IT-risk management regulatory and supervisory framework are addressed, respectively. The issues and challenges are highlighted in Section 6, and the policy recommendations are given in Section 7.

2. Overview of the Financial System

The Mongolian financial system is relatively small and simple but is growing rapidly. Like most developing economies, the financial system is dominated by commercial banks. As at the second half year-end 2007, there are 16 registered commercial banks in Mongolia. They accounted for over 95% of the total assets of the financial system (Figure 1). The total banking assets grew from 56% of GDP in 2003 to about 78% of GDP in 2007, representing nearly a four-fold increase in its nominal value (Figure 2). The ownership of the banking sector is significantly foreign-owned, but unlike the pattern in other developing countries, the foreign owners are typically institutional investors, wealthy individuals, or small regional banks.

Figure 1
Banking vs. Financial Sector

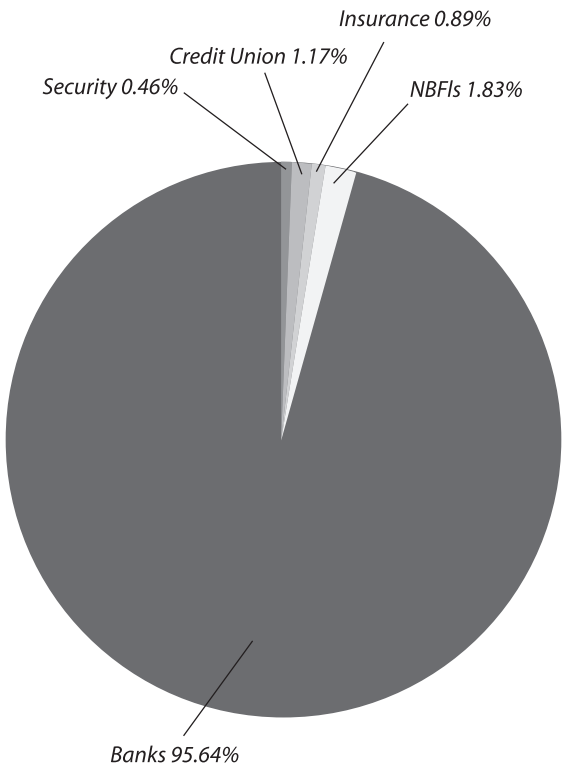
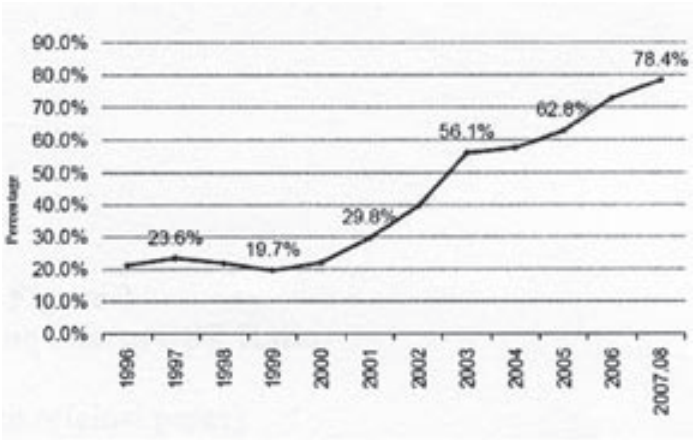


Figure 2
Total Banking Assets/GDP Ratio



The Mongolian banking system is experiencing rapid loan growth. The total outstanding loans of the banking system rose by 59.9% over the previous year, amounting to MNT 2,559.4 billion (US$2.2 billion). Bank loans to the private sector, one of indicators of financial deepening, grew by 57.1% over the previous year, and reached MNT 1,472.1 billion (US$1.3 billion). Loans to individuals grew by 67.4% to MNT 1,031.5 billion (US$0.9 billion). Loans to other entities expanded by 2.1 times to MNT 44.8 billion (US$0.04 billion). In terms of asset quality indicators, as at the second half year-end 2008, performing loans of the banking sector account for 95.0% of total loans, past due in arrears 2.1%, and non-performing loans 2.9% , respectively (Figure 3).

As at the second half year-end 2008, the capital adequacy ratio for the whole banking system, one of the main indicators of banks' capability to withstand risks, stood at approximately 14%, exceeding the central bank's requirement of 10% (Figure 4).

Figure 3
Non-performing Loans

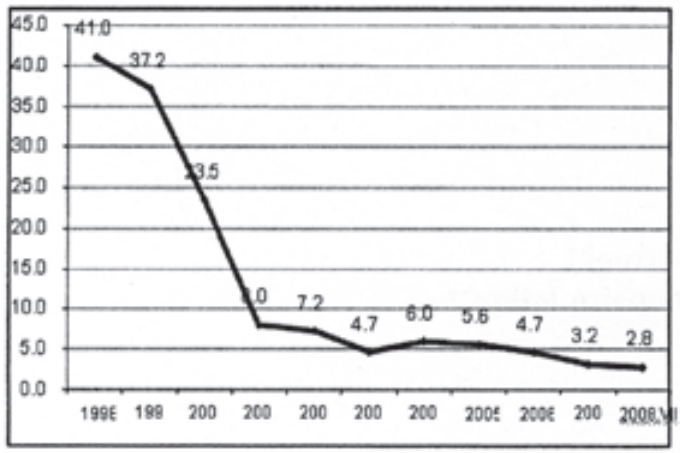
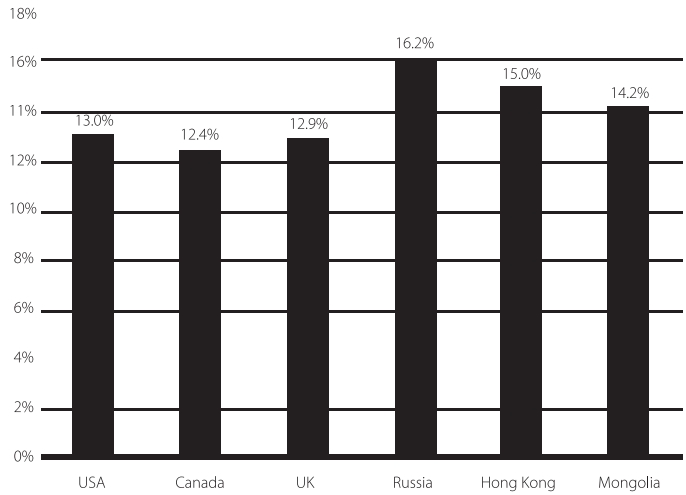


Figure 4
Capital Adequacy Ratio



The steady improvement and expansion of bank activities are reflected in the following ratios: ratio of total assets of the banks to GDP is 74.2%, ratio of total loans to GDP is 45.1%, ratio of total deposits to GDP is 32.1, and ratio of total current account balances to GDP is 13.6. Compared with the previous years, the statistics show a constantly improving tendency.

As at the end of 2007, the banking sector of Mongolia comprises 16 licensed commercial banks operating a total of 787 bank units. The number of bank units consists of 76 branches, 642 settlement centers, 13 saving units, 47 other units, eight representative offices, and one foreign exchange unit. Out of the 16 commercial banks, only three do not have a rural area network and concentrate their operations in Ulaanbaatar, the capital city of Mongolia.

3. Survey on IT Implementation

The development of technology infrastructure in Mongolia is rapid and substantial. The Information and Communications Technology Authority (ICTA) was established in 2004 to accelerate the development of the Information and Communications Technology sector and coordinate its activities. As mentioned above, the legal coordination is still important and draft laws, namely, "About e-Government", "E-signature", and "E-agreement" have been developed. In Mongolia there are three mobile phone operators and over ten Internet providers.

As a result of programmes, such as "Computer to Everybody", "One Tugrug Internet", and "Internet to Every Family," aimed at the development of information and communications education and at raising usage of the Internet, the cost of personal computers and Internet services have been reduced substantially. Out of the total population of 2.6 million in Mongolia, the ICTA, following the implementation of the above programmes, counts over 80,000 families as having acquired computers and estimates the number of Internet users exceeding 400,000.

Plans are in the pipe line to modernise the payment system to strengthen the financial system infrastructure. Year to year, the transaction volumes and values settled by the inter-bank payment system are growing strongly. The use of non-cash payment instruments, while still relatively small, has also been growing. A real time gross settlement (RTGS) for high-value transactions, to reduce payment system risks, is planned to replace the current end-of-day net settlement system in 2009. A card processing system that could replace the individual banks' proprietary systems is also scheduled to be launched. Furthermore, in conjunction with the renovation of the national payment system, a Payment Policy and Regulation Unit was established under the Bank of Mongolia in early 2008. The purpose of this Unit is to formulate the relevant policies and regulations in regard to the development of the national payment system and its further monitoring and supervision.

The findings of the survey of the status of IT infrastructure installed in the country are presented below in Figure 5.

Figure 5
Status of IT Infrastructure Installed in Mongolia

No.	Item	Yes/No
1	Communication Network	
	Cable (Phone line)	Yes
	Satellite	Yes
	Fiber Optic	Yes
	Use of Cellular Phone	
	Is it relatively wide spread?	Yes
3	Use of Internet	
	Is it relatively wide spread?	Yes
4	National Payment System	
	Operated by government agency / central bank	Yes
	Operated by an independent or private company	No
	Automated/Computerised Payment System	Yes
	RTGS	No
5	National Securities Settlement System	
	Operated by government agency / central bank	Yes
	Automated/Computerised Settlement System	No

As we can see from the survey above, although the IT infrastructure installed in the country does generally satisfy the basic requirements, the national payment and securities settlement systems still have room for improvement.

Most of the financial institutions are looking to technological innovations as instrumental in reaching out to new customers and maintaining their market share. Banks offer new products and services in the area of e-banking (mobile and Internet banking) and issue bank debit and credit cards. However, the legal and regulatory environment is still in need of significant strengthening to support these innovations. Increased use of technologies by the banks is taking place in some cases without the coverage of sufficient laws and regulations, specifically in regard to the authenticity and finality of e-transactions, verification of e-signatures, customer privacy protection, and banking information confidentiality. Currently, two statutory acts and amendment to the Civil Code regarding these subjects have been drafted by the Information Communication Technology Authority and are expected to be tabled in the Parliament in 2008.

The IT-related products implemented by banks in the Mongolian financial market are summarised in Figure 6 below.

Figure 6
IT-related Products Implemented by Banks in Mongolia

No.	Item	Yes/No
1	Credit Card	
	National (only used in the country)	Yes
	International	Yes
2	Debit Card	
	National (only used in the country)	Yes
	International	Yes
3	ATM	
	Individual bank	Yes
	Nationally-Shared ATM	No
	Internationally-Shared ATM	Yes
4	Electronic Fund Transfer (EFT)	Yes
5	EFT at Point of Sale	
	National (only within the country)	Yes
	International	Yes
6	Remittance Service	
	Domestic companies	Yes
	International companies	Yes
7	Phone Banking	
	Informational	Yes
	Transactional intra bank	No
	Transactional inter bank	No
8	Mobile/SMS Banking	
	Informational	Yes
	Transactional intra bank	No
	Transactional inter bank	No
9	Internet Banking	Yes
	Informational	Yes
	Transactional intra bank	No
	Transactional inter bank	Yes
10	Pre-paid card	

One of the main applications of technology in the banking market is the card business. The card business is expected to grow rapidly, even as it is constrained by the lack of a common platform for card processing and electronic bill payments. Most of the credit and debit card transactions are processed by the two largest banks, with another bank starting recently to develop its own card processing system. The lack of interoperability of these systems, which may become a source of weak competition, is increasingly inconvenient for consumers and vendors.

The Switch and Clearing Center at the Bank of Mongolia is considered as capable of providing a shared-card processing platform and is in compliance with the current international technical standards for card processing.

The research conducted by the Payment and Settlement Department, Bank of Mongolia on the "Usage of payment cards in Mongolia," based on the data of June 2007, highlights the following issues relating to the bank card business in Mongolia.

Out of the16 commercial banks operating in Mongolia, ten of them are engaged in the card business. There are four separate networks available in the market facilitating card transactions:

1. Golomt bank network (sub-users consisting of Zoos, Capitron and Xac banks);
2. TDB network (sub-users consisting of Ulaanbaatar, Mongol Post and Savings banks);
3. Khan bank network; and
4. Anod bank network.

Compared to 2005, as at the second half year-end 2007, the number of bank card holders (used as a tool for payment) had increased by 2.2 times from 241,000 to 538,900. Most of these are card holders of the three major commercial banks in Mongolia, namely, Golomt, TDB and Khan Bank. Comparisons of the average amount of transactions done through POS, ATM and POB terminals show that average amount of transactions done through POS has increased the most (by MNT 50,700) followed by average amount of transactions done by POB terminal (by MNT 49,000). Comparing to the data of the second half of 2006, as at the second half year-end 2007, the average amount of transactions conducted through ATM stayed the same. The reason behind the increase in the transactions performed at POS and POB terminals lies in the increased number of terminals made available at the selling points.

Analysis of the market shares of the individual banks in the card business transacted through POS terminals (based on the total transaction value) show that, as at second half year- end 2007, three major banks, namely, Golomt (37%), Anod

(29%), and Khan Bank (31%) hold equally large stakes amounting to 97% of the total market transaction values. On the other hand, the analysis of market shares of individual banks in the card business transacted through ATM (based on total transaction value) show that, as of the second half year-end 2007, TDB holds the major stake of market shares, amounting to 85% of total market transactions.

For a small country as Mongolia with a sparse population of 2.6 million) and the population concentration of over 50% living in its capital, Ulaanbaatar, the prevailing situation where each individual bank operates its own network for its card business does not facilitate the efficiency of the payment system. It impedes the convenience of customers and hinders the future development of non-cash payment instruments. The implementation and availability of a common settlement platform will improve the efficacy of ATM and POS terminals, thus further facilitating the development of bank products and the utility of customers.

Moreover, an issue of heterogeneity of the technology implemented in the financial institutions is important. In addition to IT-related products, IT related applications utilised by commercial banks are diverse and heterogenic in the level of development and sophistication.

Figure 7
Status of IT-related Applications in Addition to IT-related Products

No.	Item	Yes/No
1	Core Banking: General Ledger, Third Party Fund, Loan, and Consumer Information File	Yes
2	Treasury	Yes
3	Remittance	Yes
4	Trade Finance	Yes
5	Corporate Online Service	No

Due to the significant differences in the operation activities as well as in the level of development of banking products and services, the technology implemented by the banking institutions of Mongolia differs substantially. Banks operating extensive branch networks require heavy investments in IT infrastructure and IT-related risk management, while the smaller banks that concentrate their activities mainly in the large cities and limit their products in their core business, require less sophisticated IT-risk management procedures.

According to Mongolian Laws, rules and regulations, the senior management of the commercial banks is required to establish acceptable limits in regard to the financial and operational risks inherited in their operations, including credit, market,

operational, legal and other risks. The assignment of responsibilities and decision-making authorities should be appropriately established by the management and supported by adequate internal controls based on proper evaluation of the bank's risk profile. The Bank of Mongolia monitors the effectiveness of risk management procedures, capital and reporting requirements.

The Bank of Mongolia developed and implemented a guideline for the evaluation of operational risks by the commercial banks in 2006. Both standardised and advanced measurement approaches were prescribed, allowing the banks the discretion to choose which methodology to adopt for their risk measurement. While the large banks have more or less established their systems for the management of operational risks faced in regard to the technology-supported financial products and operations, some of the smaller banks do not yet possess the sophistication to measure and control their risks, and not all the banks have established the procedures to manage their IT risks.

The Bank of Mongolia has yet to implement IT-risk management examinations on the commercial banks. The Bank of Mongolia–JICA joint project started work in 2008 in developing the regulatory and supervisory framework of the Bank of Mongolia to cover IT examinations. The members of the project team are currently formulating the principles, policies and procedures to be followed with respect to the conduct of IT supervision by the Supervision Department of the Bank of Mongolia. The actual examinations are planned to be carried out in 2010. The major challenge for the Bank of Mongolia is to ensure the adequacy and soundness of the regulatory framework and policies to be introduced for the purpose.

4. Impacts of IT Implementation on Financial Institutions

IT implementation does increase efficiency, but it may also increase operational and IT-related risks as well as impact on stability. The implication of IT implementation in terms of the potential risks and impact on the financial sustainability should be carefully considered, and appropriate preventive measures should be taken by the financial institutions.

In 2006, the Bank of Mongolia issued a guideline on "Measuring the Operational Risk." The guideline spells out the mathematical and statistical techniques the commercial banks may use in the calculation and assessment of their operational risks.

Figure 8 below list the types of risks to be addressed and controlled by the financial institutions in meeting the requirements of the risk management framework.

Figure 8
Types of Risks

No.	Item	Yes/No
1	Operation Risk	Yes
2	Liquidity Risk	Yes
3	Credit Risk	Yes
4	Strategic Risk	Yes
5	Reputation Risk	Yes
6	Legal Risk	Yes
7	Compliance Risk	Yes

At present the banking sector does not have any minimum standard for IT risk management. The practice of operational risk assessment by the banks in regard to the IT-supported financial products and IT-supported financial institution operation is in its infancy.

While the population concentrations are in few major cities in Mongolia, the banks that operate extensive networks in the rural areas in a country as large as Mongolia, do invest substantially in IT infrastructure.

The potential risks that manifest from the implementation of IT-supported products and operations are many: risk due to disruptions, malfunctions and/or defects of computer systems; risk of financial loss from abuse of the computers; risks that the information systems strategy is inconsistent with the bank business strategy; risks that information system investments and technology become obsolete; risks of the banks' financial position weakening due to cost increase; risks that the usability, effectiveness and quality of the information systems deteriorate due to the delay of servicing, failure of development, and/or introduction of information systems; and other risks.

It is important that the prevailing IT supervisory framework to be implemented in the future should take into consideration the assessment of the above risks from the standpoints of the financial institutions and the Bank of Mongolia.

5. Prevailing IT Supervisory Framework and Regulations

In view of the potential impact of IT implementation on the financial institutions, it is important that respective regulatory authorities implement the supervisory framework to measure and control the IT risks. The Bank of Mongolia has yet to implement the requirement of IT risk-management examinations on the commercial banks.

However, the Bank of Mongolia–JICA joint project has started work in 2008 in developing the supervisory framework of the Bank of Mongolia to include IT examinations. The members of the project team are currently formulating the principles, guidelines and manuals, policies and procedures to be followed with respect to the conduct of IT supervision by the Supervision Department of the Bank of Mongolia. The actual examinations are planned to be carried out starting in 2010. The major challenge for the Bank of Mongolia is to ensure the adequacy and soundness of the regulatory framework and policies to be introduced for the purpose.

The draft regulation on bank IT-risk examination sets out the following principles:

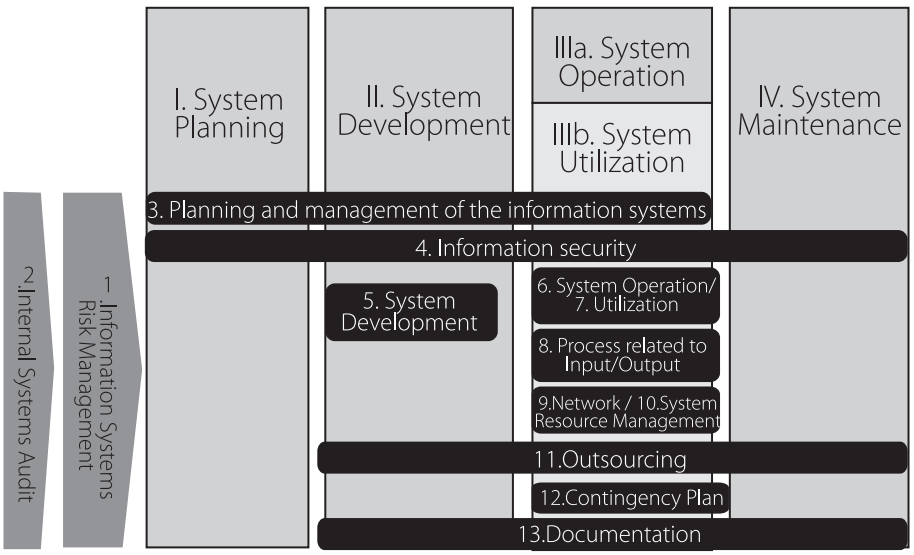
- Inspection reinforces discipline by the market and by others assuming the responsibility of internal management and by fair external audit by the accounting auditor;
- Assuming that information system risk is one of the core risks of the financial institutions' business, the management of the financial institution is responsible for leading the development and establishment of internal management systems to control the information systems risks;
- On inspection, the supervisors shall check the systems for compliance with the prevailing laws and regulations, and risk management shall focus on process checking. The examination of the effectiveness of information system risk management shall be the prior concern.

The main purpose and underlying philosophy of the Bank of Mongolia for implementing IT inspections shall be insuring the appropriate implementation and effectiveness of the IT risk management goal of the financial institution. While the IT risk management goal shall be set as "attaining the objectives of IT", the objectives of IT shall include: effectiveness, efficiency, creditability, security and compliance of IT systems of the bank.

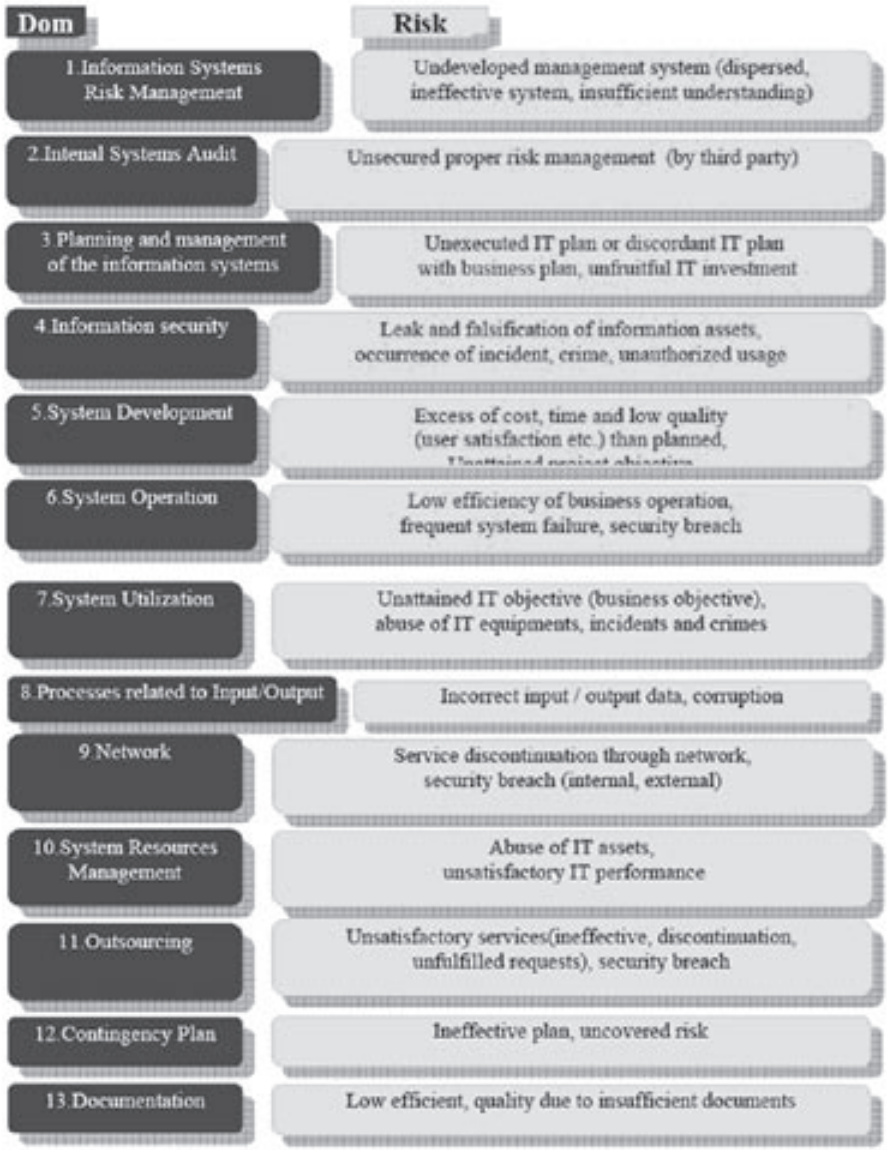
The proposed regulatory framework for IT supervision being developed by the Bank of Mongolia, working in conjunction with the JICA, include (i) IT inspection guideline, (ii) IT inspection manual (iii) IT inspection handbook and (iv) IT inspection standards. Based on the above documents, checklists are developed for the purpose of assisting the examiners to evaluate the compliance of IT procedures and risk management at the bank against the standards set by these regulatory documents. In these regulations, the inspection domain proposed, which is structured following the system lifecycle, is inclusive of the following areas:

Figure 9

Inspection domain and System Lifecycle



Risks that are to be recognised within each of the inspection domains are summarised in the diagram below:



The status of the IT supervisory framework that is in progress to be implemented in the banking sector by the Bank of Mongolia is indicated in Figure 10 below.

Figure 10
Status of IT Supervisory Framework

No.	Item	Yes/No
1	Is IT Implementation reported regularly?	About to
2	Is IT audit conducted?	Yes
	By bank/IT supervisors from supervisory authority	
	Off-site	No
	On-site	Yes
	By internal or external (third party) auditors (on-site)	No
	Special IT audit/examination outside regular examination (on-site)	No
3	Does the formal framework exist[1]?	Yes
4	If yes, is it stipulated in a regulation?	No
5	Is there minimum requirement in IT Implementation?	No
	Are the following items implemented: Active supervision by Top Management (IT Steering Committee)	Yes
	IT Policy and Standard Operating Procedure	Yes
	IT risk is included in the risk-based management	Yes
	System development life cycle	
	All layers of IT system	Yes
	Internal control system for IT Implementation	Yes
	Business Continuity Plan and Disaster Recovery Plan	Yes
	Periodical IT audit (internal/external)	Yes
6	Because it involves supervision procedure, is IT outsourcing especially regulated?	Yes
7	Because it involves consumer protection, is E-banking products especially regulated?	Yes
8	Are any IT-related laws (cyber law, e-commerce, m-commerce, digital signature) installed?	No

1 On very initial, implementation starting level

Figure 11 below specifies the coverage and proposed regularity of future IT inspections to be conducted by the Supervision Department of the Bank of Mongolia.

Figure 11
IT Audits

No.	Item	Yes/No
1	Is it conducted regularly?	Not yet
2	If not regularly, is it conducted case by case?	No
3	If regularly, objects of audit:	
	Organisation and Management	Yes
	System development process	Yes
	Operation	Yes
	Software and Application, including E-Banking	Yes
	Security (authentication, authorisation and protection – including audit trails, encryption)	
	BCP/DRP	Yes
	Communication Network	Yes
	Outsourcing process	Yes
	Internal Auditing	Yes

It is important to mention that the Bank of Mongolia presently does not have any IT-specialised supervisors/auditors. Its human resource capability is still one of the major issues to be addressed. However, in future, the Bank of Mongolia plans to upgrade the competence of its financial auditors and to equip and gear up some of them to specialise in IT audits. The IT supervisory training has been acknowledged as an important step to be taken. Mongolia at this point of time does not have any structured/comprehensive training for auditors specialising in IT. Thus, there is no standard qualification for IT auditors. The teams of selected on-site examiners work closely with Japanese experts on each of the requirements specified in the proposed manual for the members to specialise in the relevant areas. Trial on-site examinations had been conducted at one of the largest bank in the end of 2008. From the preliminary results, it can be seen, that although a comprehensive framework for conducting IT operations had been established, within the bank examined, the information system risk management and information system audit functions have not been fully established, and are not fully in compliance with the best practices proposed in the current draft regulations of the Bank of Mongolia. The information security policies and procedures are to be more thoroughly addressed.

Coordination among the financial institution authorities is also one of the important issues to be addressed in the future. The Bank of Mongolia is not the authority regulating the NBFIs. Thus, coordination in controlling IT risks within the framework of the financial system stability is essential and important. The current developments in coordination between the regulatory authorities for the financial market participants include, among other things, a Memorandum of Understanding entered between the Bank of Mongolia and the Financial Regulatory Authority, with the purpose to conduct consolidated inspections of financial organisations and to share related information when needed. The Financial Stability Council has been also established by the joint decree of the Bank of Mongolia, the Ministry of Finance and the Financial Regulatory Committee (FRC) in 2007. The mission of the Council is to contribute to sustainable economic growth through the development of a sound and competitive financial infrastructure and improvement of the financial services in terms of quality and access. The Financial Stability Council aims to co-operate closely with the other international financial institutions and promote the competitiveness of the Mongolian banking and financial sectors in the international markets.

6. Issues and Challenges

As we can see from the analysis above, the financial institutions vary in their scale and business characteristics and the specific measures adopted by them to control IT risks differ. A uniform risk management system does not exist as yet in Mongolia. Based on the proposed IT risk-management framework, the management of the financial institutions is expected to develop their own corporate policies and regulations in accordance with the scale and business characteristics of their organisation.

There is a compelling necessity for the development of adequate IT Infrastructure. Against this pressing need, the establishment of a proper legal environment to support IT risk management (inclusive of the enactment of IT security-related laws, customer privacy requirements in Internet banking), establishment and enforcement of minimum standards for IT risk management in the financial sector, improvement of the level of awareness of IT risk at Board level, establishment of standard qualifications for IT auditors and the improvement of supervision with technology skills, are yet to be done.

For the Bank of Mongolia, the introduction of sound policies and adequate regulatory framework for the implementation of IT supervision is major challenge to be addressed in the near future. The success of the Bank of Mongolia's IT supervision is determined by the extent to which it is able to attain its objective

of overseeing the performance by the executive management of the financial institutions fulfilling their role in building risk management systems within their organisations.

Where proper risk management systems are not put in place, the responsibility between the Board of Directors and the Executive Management of the financial institutions will be blurred, with the result that it will give rise to perception gaps with regard to the definition and delegation of the scope, responsibility and authority of operations.

With further development of the economic and financial sector in Mongolia, as well as with the economic integration of the region, the issues and general principles for supervision of e-banking – like for instance, compatibility for cross-border supervision, home-host responsibilities, bilateral agreement for information-sharing - will be among the important concerns. The policies and procedures proposed in the current IT risk management framework for the financial institutions should incorporate the implementation of internationally acceptable practices and procedures. The following issues relating to risk management for electronic banking, inclusive of board and management oversight, security controls, legal and reputational risk management as well as issues on cross-border e-banking, including home-country oversight on a consolidated basis and host-country oversight activities within its local market, are still to be addressed.

7. Recommended Policy

From the analysis above, it can be concluded that, based on purpose and technological sophistication, the adoption of IT technology in banking sector in Mongolia can be characterised as entering the second stage where IT is used as an engine for financial development. Although the introduction of electronic payment systems and e-banking services (Internet banking, phone banking, ATM, etc.) is still in the early stage and is set to take off in the future, it is crucial that the impact of technological innovations be understood not only by the financial institutions, but also by regulatory bodies because of their implications for the regulation and supervision of the banking and financial sector.

For Mongolia, the finalisation and implementation of IT inspection in the banking institutions (and in the NBFIs in future) and the education of Top Management in IT risk awareness are the key priorities. The implementation of the proposed policies and regulations, and the proposal specifying the minimum requirements for IT risk management at each stage of the information system lifecycle are the first steps towards the development of the IT risk-management

standards in system planning, development, operation, utilisation and maintenance. The assessment of the sustainability of the financial institutions, within the risk-based supervision framework of the Bank of Mongolia, should integrate not only the financial risks but also the operational and inherent IT-related risks and their management by the institution.

Further, based on the main findings and issues raised from the regular IT inspections, the minimum requirements for IT implementation, IT supervisory framework, and the deployment of IT auditors in both the financial institutions and in the Bank of Mongolia are required to be introduced. Additionally, the requirements for the financial institutions to structure their information security and risk management programmes and practices for securing their information assets are to be implemented.

It is essential for the Bank of Mongolia to do capacity building and equip its examiners with the technical skills for them to understand IT-related risks and facilitate its examiners to acquire the necessary qualification to become IT auditors.

The regulatory authorities in coordinating to introduce the above-mentioned standards should extend the implementation of these standards to all the financial institutions, and not just banks. The awareness and control of the IT-related risks should be implemented within the banking institutions and should also be implemented for compliance by the other financial institutions.

And lastly, as aptly put by Dr. Haibin Zhu, during the SEACEN Workshop on "The Supervisory Impact of Technology on SEACEN Financial Institutions: Issues and Challenges" in Kuala Lumpur, Malaysia, 11 November 2008: "We are in a time of rapid change, and we must continue to adapt. But at the same time, we must not lose sight of the fundamental elements of banking supervision." (Nout Wellink, 4 October 2006).

References

BoM-JICA Joint Project on "Introducing IT Inspection to the Supervisory Framework of the Bank of Mongolia," IT Inspection Guideline Draft Paper, 2008.

BoM-JICA Joint Project on "Introducing IT Inspection to the Supervisory Framework of the Bank of Mongolia," IT Inspection Manual Draft Paper, 2008.

BoM-JICA Joint Project on "Introducing IT Inspection to the Supervisory Framework of the Bank of Mongolia," IT Inspection Standards Draft Paper, 2008.

The Center for Financial Industry Information Systems (FISC), Japan, "Information System Audit Guidelines for Banking and Related Financial Institutions," 2008.

6th ASOSAI Research Project, IT Audit Guidelines, 2003.

Federal Deposit Insurance Corporation (FDIC), Information Technology Risk Management Program – New IT Examination Procedures, 2005.

BCBS, "Risk Management Principles for Electronic Banking," 2003.

BCBS, "Management and Supervision of Cross-Border Electronic Banking Activities," 2003.

BCBS, "Sound Practices for the Management and Supervision of Operational Risk," 2001.

CHAPTER 6

THE SUPERVISORY IMPACT OF TECHNOLOGY ON SEACEN FINANCIAL INSTITUTIONS: ISSUES AND CHALLENGES IN MYANMAR

by Khin Cho Cho[1]

1. Introduction

Information and Communication Technology (ICT) has made much progress with the digital revolution. Many countries in the region are in the early stage of introducing and applying ICT in their businesses and activities. Our neighbouring countries are making much use of the latest information technology with much benefit. This technology is very important and useful in a country's financial system because of its timely dissemination of useful information.

The development of information technology and computer usage in Myanmar started in early 1980s. In 1985, under the Project of the United Nations Development Programme (UNDP) for Human Resource Development, the computer training courses jointly sponsored by Central Statistical Organisation (CSO) and UNDP were given to government staff from the various ministries while the University of Computer Science had been providing ICT-related courses. In the late 1980s, the Central Statistical Organisation installed Mainframe 1BM 4318 for data processing and analysis. Since then personal computers were widely used among the government agencies.

In the banking sector, after promulgation of the Central Bank of Myanmar Law, the Financial Institutions of Myanmar Law and related Rules and Regulations of the said laws, which are in harmony with the market-oriented economic system, domestic private banks were inaugurated in 1992 providing banking services by using modern techniques. From that time on until today, computers are used significantly in the banking sector and software application introduced.

While most of the countries have been making wide use of the latest information technology in the banking sector, Myanmar has only recently introduced IT in a limited manner in the areas of deposit taking, lending, accounts management, and internal remittance. Banking network between the

1 Author is Assistant Director of the Internal Audit and Bank Supervision Department of Central Bank of Myanmar. The views and recommendations expressed here are those of the author and do not necessarily reflect that of the Central Bank of Myanmar.

Central Bank of Myanmar and all the banks is now in the initial stage for the purpose of reporting system services and fund transfer within a country. Besides these activities, no new IT- related financial products and services have been implemented yet. But the plan for implementing these products and services is under consideration.

This paper purposes to give a very brief account of the IT activities in Myanmar. It will highlight some of the issues and challenges that we encounter and conclude with some suggestions as to how we should address the issues and challenges.

As we have not made much progress in the implementation of IT-related products and services in banking sector, we can only make a general presentation of the issues and challenges. As we progress with IT implementation, we shall be in a better position to bring the issues and challenges we are facing into clearer focus.

2. Overview of the Financial System

2.1 Brief Introduction to the Financial Sector

The present structure of the financial system can be divided into two main sectors: Banking sector and Non-banking sector. The banking sector consists of the Central Bank, four state-owned banks, six domestic private banks and nine semi-private banks, and they are as follows:

2.1.1 Banking Sector

(a) The Central Bank of Myanmar (CBM)
(b) State-owned Banks
    (1) Myanma Economic Bank (MEB)
    (2) Myanma Foreign Trade Bank (MFTB)
    (3) Myanma Investment and Commercial Bank (MICB)
    (4) Myanma Agricultural Development Bank (MADB)

(c) Domestic Private Banks
    (1) Yoma Bank Ltd.
    (2) Kabawza Bank Ltd.
    (3) Myanmar Oriental Bank Ltd.
    (4) First Private Bank Ltd.
    (5) Tun Foundation Bank Ltd.
    (6) Asia Yangon Bank Ltd.

(d) Semi-Private Banks
    (1) Co-operative Bank Ltd.
    (2) Innwa Bank Ltd.
    (3) Myawaddy Bank Ltd.
    (4) Myanmar Citizens' Bank Ltd.
    (5) Myanmar Industrial Development Bank Ltd.
    (6) Myanmar Livestock and Fisheries Development Bank Ltd.
    (7) Sibin Tharyaryay Bank Ltd.
    (8) Yadanabon Bank Ltd.
    (9) Yangon City Bank Ltd.

2.1.2 Non- banking Sector

(a) Myanma Insurance, with 38 branches.
(b) Myanma Small Loan Enterprises, with over 200 branches.
(c) Myanmar Oriental Leasing, which is an affiliate of Myanmar Oriental Bank Ltd., and conducts hire purchase and leasing business.
(d) 13 Foreign-bank Representative Offices as liaison offices.
(e) Government financial organisations:
    (1) Budget Department
    (2) Internal Revenue Department
    (3) Customs Department.

Among the state-owned banks, the Central Bank of Myanmar, the central bank, is responsible for licensing, inspecting, supervising and regulating financial institutions and prescribing such directions as may be necessary to ensure the solvency and soundness of such institutions with the main objectives of bank supervision, such as protection of depositors' funds, monetary stability and efficiency of the financial institutions. The Myanmar Economic Bank (MEB), with 318 branches, provides nationwide commercial and development banking services, and it has been allowed to deal in foreign exchange business since April 1996. The Myanmar Foreign Trade Bank (MFTB) offers foreign banking facilities (international trade transaction facilities) in conjunction with 143 correspondent banks throughout the world. The Myanmar Investment and Commercial Bank (MICB) conducts both domestic banking and foreign banking activities through a correspondent network of 166 banks. The Myanmar Agricultural Development Bank (MADB) provides rural development banking services with the objectives not only to support socio-economic development, but also to encourage saving habits in order to nurture the spirit of self-help among the rural population. The MADB was transferred to the related ministry, the Ministry of Agriculture and Irrigation in 1996 to improve its efficiency and effectiveness.

Among the domestic private banks and semi-private banks, First Private Bank, Myanmar Industrial Development Bank, Myanmar Livestock and Fisheries Development Banks, Myanmar Citizens Bank and Co-operative Bank are partially state-owned. Except for two banks which provide commercial banking facilities, 13 banks conduct investment and development banking services. One leasing company, the Myanmar Oriental Leasing, engages in hire purchase and leasing business. (See Annex 1).

2.2 IT-related Products and Services in the Banking Sector

Before 2003, five major domestic private banks were allowed to introduce ATM, Credit Card, and Point-of-Sales services to a certain extent. Myanmar May Flower Bank Ltd. was allowed in early 2000 to introduce ATM for their staff and customers , with the provision of facilities limited to cash withdrawal and account balance inquiry in Yangon and Mandalay only. Another four banks, namely, Myanmar Oriental Bank, Yoma Bank, Asia Wealth Bank, Kanbawza Bank Ltd., and Myanmar May Flower Bank, were allowed to provide Credit Card and Point-of-Sales facilities by using on-line system as well as telecommunication channel in some major cities during the period 1994 to 2003. The private banks have been operating smoothly, giving excellent services to the public and are making profits. The supervision and regulation of these institutions were undertaken by the on-site examination team in accordance with the normal procedure prescribed by the CBM.

Despite the development of the banking sector, the general public preferring higher returns for their savings, opted to deposit their money in companies or firms outside the banking sector. These companies or firms were operating illegal financial activities and when they collapsed, it triggered a run on the banks as the people, worried about the safety of their money, withdrew massively their deposits from the banks. This caused some large banks to face a liquidity crunch, but it did not spread to all the banks. In solving these difficulties, the Central Bank provided liquidity support to the problem banks and measures were taken to recover the banking sectors. Since then, the new financial products and services were banned and they had not been allowed to resume.

Two banks, namely, Asia Wealth Bank and Myanmar May Flower Bank, have ceased business operation and had their banking licenses withdrawn on 1st April 2005 due their non-compliance with the existing Financial Institutions of Myanmar Law (FIML), Moreover, the Myanmar Universal Bank's license was also withdrawn by the CBM on 1st August 2005 because this bank was not

operating in compliance with the Control of Anti-Money Laundering Law and FIML as well. The Yoma Bank Ltd. is prohibited from taking deposits and making loans but is allowed to undertake internal remittance only.

At present all the domestic and semi-private banks are permitted to engage only in domestic and core banking services, but not in international banking operations. A few banks are conducting their branch banking business via on-line network services which are outsourced to the private-service providers. Some other banks are offering the computerised banking services. So far, IT-supported financial products and services have not been implemented. The Central Bank of Myanmar has a plan to allow banks to gradually introduce IT-supported financial products and services, yet to date the same have yet to be introduced.

In the banking system, the State-owned banks account for 85% of the total banking assets. After the banking turbulence of early 2003 due to the illegal operation of general services enterprises, the Central Bank of Myanmar closely monitored the private banks, prescribed instructions and took the necessary actions under the guidance of the Central Supervision Committee and the Bank Supervisory Committee. As the result, the banking sector become stable and gained much progress. The total assets of the banking sector and the amount of loans have since increased and the NPL ratios have also declined. (See Annex 2).

2.3 Supervision and Regulation of Financial Institutions

The Central Bank of Myanmar is empowered to inspect, supervise and regulate the financial institutions by the Central Bank of Myanmar Law Section 8(f) and the financial institutions are inspected by the Central Bank according to the Financial Institutions of Myanmar Law Section 48. The Central Bank of Myanmar supervises and regulates the banking sector with the main objectives of safeguarding the interest of depositors and promoting monetary stability and efficiency of the financial institutions.

In this respect, the Bank Supervision Department of the Central Bank of Myanmar undertakes the on-site examination of the domestic private banks on a routine basis and off-site monitoring to achieve the above objectives.

The Central Bank of Myanmar has issued relevant guidelines which consist of the following:

(1) Statutory Reserve Requirement
(2) Capital Adequacy
(3) Liquidity
(4) Classification of NPLs and Provision of Bad and Doubtful Debts
(5) Security-wise and sector-wise of loan conditions.

The Central Bank has also been taking regulatory action by applying the following prudential provisions:

(1) Minimum Reserve Requirement
(2) Liquidity Control
(3) Capital Adequacy Ratio
(4) Legal Lending Limits.

There are nine inspection teams with each team consisting of four members headed by a staff officer. On-site examinations are conducted in accordance with the inspection schedule on an annual basis. Inspection teams carry out their duties in accordance with the inspection manual prescribed by the Bank Supervision Department.

The off-site operations are based on the following reports which banks are required to submit to the Central Bank of Myanmar:

(1)	Weekly	(a)	Weekly reserve position
		(b)	Liquidity ratio
		(c)	Cash in hand
(2)	Monthly	(a)	Monthly balance sheet
		(b)	Income and expenditure statement
		(c)	Capital adequacy ratio
(3)	Quarterly	-	Non-performing loan statement
(4)	Annually	-	Annual report

At present, the situation of the financial sector in Myanmar, particularly in the banking sector, is now relative stable and this stability is progressing with time. Consequently, the amount of capital as well as deposits and loans have increased. The public confidence in the financial system has also progressed.

2.4 Heterogeneity / Homogeneity of the Technology

In the banking sector, the MEB is the largest state-owned commercial bank with a network of 318 branches operating in the major cities throughout the country. It provides core banking services manually. It performs the banking

operations and compilation of data with the use of personal computers. Because of its numerous branches stretching far into the remote areas, the MEB is not able to use the on-line system and its branches carry out their banking operations manually. Only a few of the domestic private banks are operating their banking business by use of the on-line system. They are using different types of application software systems developed by the local software companies for their core banking functions. Other domestic banks offer the traditional banking business and perform the compilation of data manually and use standalone computer. The transmission of data are done by using telephone lines or telex machines.

3. Survey of IT Implementation

3.1 ICT Development in Myanmar

The Ministry of Communications, Posts and Telegraphs has been responsible for the development of IT in Myanmar. The Myanma Posts and Telecommunications (MPT) is the sole operator for all telecoms and ICT facilities in Myanmar.

To enhance the long distance telecommunication and long distance telephone services in the border areas, domestic satellite earth stations were implemented in 1991 and VSAT system was introduced later. Currently 10 VSAT stations and one DOMSAT station are in operation in the rural areas. All the domestic earth stations and VSAT are linked with THAICOM 3. Broadband Satellite System has been implemented since 2004 and encouraging already the use of about 550 satellite terminals for voice and broadband data through IPSTAR. IPSTAR, designed for two-way broadband communication over the IP Platform, fully supports Internet connection and other applications for them to be used over the IP Platform. The ADSL system is also available starting from early 2006 in Myanmar. ADSL provides a complete portfolio of digital subscriber line technologies to end-users over existing copper telephone wire infrastructure.

The connection of ADSL is extended to every township for improving Internet access. 400 public Internet services centres have been projected to be introduced in 324 townships within three years to facilitate communication link.

Data communication with Packet Switching system as well as Internet services as the main infrastructure have been introduced. For international communication, Standard A Satellite Earth Station has been implemented and it is connected with SEA-ME-WE optical fibre transmission system.

Myanmar is now operating 1644 circuits to 11 countries by satellite communication as well as international optical fibre communication system. Myanmar is now participating in linking with the member countries of the Greater Mekong Sub-region and also cross-border connection with China and Thailand are being developed. Under the GMS Information Super Highway Implementation Project, the transborder fiber link between Myanmar and the PRC was opened in March 2008, and bandwidth capacity 10 Gb (STM-64) can now be used on the link and 2.5 Gb(STM-16) on its micro link. The transborder fiber optic link between Myanmar and Thailand can also be used in the Northern Part of the Myanmar border and the Southern Part of the border link will soon be opened.

Cellular Mobile Telephone System was started in 1993 and CDMA Wireless Local Loop (WLL) and GSM have been introduced in 2000 and 2002, respectively. Mobile Phone availability is very limited in Myanmar and the level of the usage of mobile phone is quite low compared to other SEACEN member countries.

At present in Myanmar, MPT and Myanmar Teleport, which are under control by the Ministry of Communications, Posts and Telegraphs, are service providers on voice, as well as e-mail, web-hosting, web-browsing, server-co-location, FTP and Internet services. MPT has an on-going project to lay down a fiber optic backbone which can provide optimum connection for high-speed networks for ICT. It is also providing mobile Internet service and e-mail service on its GMS system using GPRS Technology. MPT provides Internet services to some government agencies and private companies since 1998. Also Myanmar Teleport which offers Internet and e-mail facilities to the public since 2002 using digital telephone lines, initially deployed Broadband IP satellite from a Central HUB site in Yangon and via dial-up access. It has also deployed Fixed Broadband WLL in the two major cities (Yangon and Mandalay) since late 2002. Myanmar Teleport is also providing virtual private network services for domestic banks, government departments, private companies and a VOIP gate way.

The Myanmar Information and Communication Technology (MICT) Park, now known as Myanmar Info-Tech, a consortium consisting of over 50 local ICT companies, was inaugurated in January 2002 with the aim of leveraging the development of ICT. There are currently 30 software companies operating there.

Since 2003, Cyber Cafes are available for public use in the major cities but this facility has not reached the rural areas. The Government offices and big companies can use the Internet access very easily. All government offices and some large corporations by using domain names for e-mail address and website have become very popular today. To improve Internet access, connections of ADSL Line are being extended to every township. Recently the number of Internet users in Myanmar has reached nearly 400,000, up from 9,255 in 2004/05, according to the MPT and Myanmar Teleport Statistics. Moreover, the three -year project which started in 2006/07 has been carried out to establish 400 public access centers in 324 townships of ten major cities, namely Yangon, Mandalay, Pyinmana, Pyay, Magway, Muse, Myitkyina, Monywa, Pathein and Taunggyi, within three years to facilitate communication links. However, the ratio of total Internet users against total population is 0.70% and the ratio is quite low amongst the member countries.

Cyber Laws (Electronic Transaction Law) was enacted in April 2004 to provide a suitable legal framework for ICT development. Communication Law which will cover all aspect of Telecommunication and ICT, is in the drafting stage under the guidance of the Myanmar ICT Development Council, the highest body for ICT in Myanmar. The government organisations and the ICT companies are working towards the development of ICT through various projects consisting of e-passport, smart card, smart school, certification authority, e-procurement, e-government, e-education and e-learning. E-National Task Force and four working groups were formed in 2000 and they are responsible for leading the ICT development activities. The government has planned for the of installation of new telecommunication networks as well as the upgrading and modernisation of the existing services to meet the public demand.

There are 22 universities offering computer studies and computer science. throughout the country providing ICT education courses.

In the banking sector, the Myanmar Economic Bank (MEB), the largest State-owned commercial bank, has 318 branches throughout the country and it conducts its banking operation by using personal computers with accounting application software as well as manually. It communicates with its branches and transmits data and information and transfer of fund by using telephone line or telex or fax.

Only the three largest domestic private banks, namely, the Yoma Bank Ltd, Kanbawza Bank Ltd. and the Cooperative Bank Ltd., are conducting data transmission and funds transfer among their branches through on-line network by using VSAT and IPSTAR. The other banks are linked with their branches through telephone line or telex or fax for transmission of data and information as well as for the transfer of funds.

The following survey table shows the status of IT infrastructure installed in Myanmar.

Figure 1
Status of the IT Infrastructure Installed in Myanmar

No.	Item	Yes/No
1.	Communication Network Cable (Phone line) Satellite Fiber Optic	Yes Yes Yes Yes
2.	Use of Cellular Phone Is it relatively wide spread?	Yes No
3.	Use of Internet Is it relatively wide spread?	Yes No
4.	National Payment System	Yes
5.	Operated by government agency/Central Bank	Yes
6.	Operated by an independent or private company	No
7.	Automated/computerised payment system	Yes
8.	RTGS	No
9.	National securities settlement system Operated by government agency/Central bank Automated/computerised settlement system	 Yes No

Source: Survey conducted for this research paper.

As mentioned earlier in Chapter 2, IT- supported financial products and services have not been implemented yet.

The presence of technology-supported financial products and services are mentioned below:

Figure 2
Technology-supported Financial Products and Service

No.	Item	Yes/No
1.	Credit Card National (Only used in the country) International	No No No
2.	Debit Card National (Only used in the country) International	No No No
3.	ATM Individual Bank Nationally-shared ATM Internationally-shared ATM	No No No No
4.	Electronic Fund Transfer (EFT)	Yes
5.	FT at point of Sale National (Only within the country) International	No No No
6.	Remittance Service Domestic Companies International Companies	Yes Yes No
7.	Phone Banking Informational Transactional intra bank Transactional intra bank	No No No No
8.	Mobil/SMS Banking Informational Transactional intra bank Transactional intra bank	No No No No
9.	Internet Banking Informational Transactional intra bank Transactional intra bank	No No No No
10.	Pre-paid card	No

Source: Survey conducted for this research paper.

Most of the domestic private banks are using different types of software application which are outsourced to domestic private service providers for conducting their core banking services. The status of IT – related Applications in addition to IT – related products is mentioned below.

Figure 3
Status of IT-related Applications in Addition to IT-related Products.

No.	Item	Yes/No
1.	Core Banking General Ledger, Third Party fund, loan and consumer	-
2.	Treasury	Yes
3.	Remittance	-
4.	Trade Finance	-
5.	Corporate Online Service	-

Source: Survey conducted for this research paper.

3.2 National Payment System

All state-owned banks are providing international payment and settlement system services through the Society for Worldwide Inter-bank Financial Telecommunication (SWIFT). It is an ADSL system and the Central Bank of Myanmar has been implementing SWIFT system since 2004 with the correspondent network of over 40 banks. The services consist of international payment and settlement, funds transfers and exchange of financial information.

The only way for foreign banks to have a presence in the country is to open a representative office for information and marketing purpose. The domestic private banks have not opened branches outside Myanmar and they are not allowed to operate foreign banking services and international fund transfer. Both representative offices of foreign banks and domestic private banks cannot operate the international payment services.

Another payment system is the Clearing House Mechanism. The Clearing House for cheque clearing among banks is conducted at the Central Bank of Myanmar. The Clearing and payment settlement are based mainly on manual procedures.

For inter-bank funds transfers and payment, private banks conduct them among their branches through on-line system or telex or telephone or fax depending on their availability of telecommunication network.

The banking network is now going to be implemented and it is in the initial stage for the purpose of inter-bank funds transfer and reporting system services between CBM and all banks. Moreover, the Auto Clearing System is projected to be introduced in the near future.

4. Impact of IT Implementation on Financial Institutions

To date, IT-supported financial products and services have not been introduced in Myanmar. Three of the 15 domestic private banks have provided on-line banking services including data compilation, fund transfer, account information, producing statements, internal remittance and historical transactions. So far, operational risk arises in their operations but it has not seriously affected banking operation because of the implementation of internal checks and management system, segregation of duties, proper control and password management, and on-going monitoring system.

A cyber law legislation (Electronic Transaction Law) was enacted on 30th April 2004 and the Law covers the areas of electronic signature, computer crime, electronic fund transfer and data protection. However, it does not cover all the issues arising from the implementation of IT- supported financial products and services, hence there will still be a need to widen the scope of the cyber law.

The following risks shown in Figure 4 are bound to occur.

Figure 4
IT Risks

No.	Item	Yes/No
1.	Operation Risk	Yes
2.	Liquidity Risk	Yes
3.	Credit Risk	Yes
4.	Strategic Risk	
5.	Reputational Risk	Yes
6.	Legal Risk	Yes
7.	Compliance Risk	Yes

Source: Survey conducted for this research paper.

If and when all the banks implement IT in their banking operations and introduce IT-supported financial products and services, the Central Bank of Myanmar should follow the principles of risk management for electronic banking issued by the BIS in an appropriate manner. Banks also should develop risk management procedures to control and mitigate risks associated with the implementation of IT products and services.

5. Prevailing IT Supervisory Framework and Regulations

5.1 Principles

There is no specific regulatory framework that supports the development of IT in the banking sector. The existing laws, rules and regulations do not cover the supervision of IT-supported financial products and services. However, if and when IT-supported financial products and services are introduced in the banking sector in the near future, the Central Bank of Myanmar should establish the supervisory framework to achieve the following objectives:

(a) Providing safeguards for the protection of depositors/customers,
(b) Ensuring the Central Bank's ability to promote monetary stability;
(c) Promoting the efficiency of financial institutions;
(d) Ensuring sound and safe banking sector development;
(e) Promoting efficient payment mechanism;
(f) Monitoring and controlling risks relating to the implementation of e-banking; and
(g) Ensuring all banks operations comply with the existing laws, rules and regulations as well as Anti-money Laundering Law.

5.2 Regulatory Framework and Regulations.

Currently, the Central Bank of Myanmar Law, the Financial Institutions of Myanmar Law and the related rules and regulations, together with the instructions issued by the Central Bank, are being used as a framework for overseeing banks. Therefore, these laws, rules and regulations should be subject to review and amendments in accordance with the changing environment of IT implementation.

However, the Central Supervision Committee led by the Minister of Finance and Revenue and the Banks Supervisory Committee led by the Deputy Minister of Finance and Revenue have already been organised, and these committees will provide the necessary guidance and needed actions for the supervision and regulation of the core banking operations of banks.

For the promulgation of new laws and regulations in regard to the supervision of IT implementation in the banking industry, Myanmar may require technical assistance from the international financial institutions or regional financial institutions in formulating a comprehensive Cyber Law legislation. Moreover, if Internet banking is introduced, the new laws should cover all the related future needs.

The status of IT Supervisory framework in the Myanmar banking system is as follows. Some banks which are operating their core banking activities using IT are conducting the auditing and supervision of their operations by their own programmes.

Figure 5
Status of IT Supervisory Framework

No.	Item	Yes/No
1.	Is IT Implementation reported regularly?	Yes
2.	Is IT audit conducted?	No
	By bank / IT supervisors from supervisory authority	No
	Off-site	No
	On-site	No
	By internal or external (third party) auditors (on-site)	No
	Special IT audit / examination outside regular examination (on-site)	No
3.	Does the formal framework exist?	Yes
4.	If Yes, is it stipulated in a regulation?	No
5.	Is there minimum requirement in IT implementation?	No
6.	Do the following items implemented? Active supervision by Top Management (IT Steering Committee) IT Policy and Standard Operation Procedure IT risk is included in the risk- based management System development life cycle All layers of IT system Internal control system for IT implementation Business Continuity Plan and Disaster Recovery Plan Periodical IT audit (internal / external)	 Yes Yes No No No Yes No No
7.	Because it involves supervision procedure, is IT outsourcing especially regulated?	No
8.	Because it involves consumer protection, is e-banking products especially regulated?	No
9.	Are any IT-related laws (cyber law, e-commerce, m-commerce, digital signature installed?	Yes

Source: Survey conducted for this research paper.

5.3 References / Orientation for the Prevailing Supervisory Framework

The Central Bank needs to develop the regulatory framework precisely with reference to the best practices applied by other countries. Moreover, risk assessment, management, monitoring and controlling have to be implemented.

5.4 IT Supervisory and Audit Practices

The Bank Supervision Department conducts only on-site examination and off-site monitoring of the core banking operations of the banks. On-site examination can only be conducted once a year because the institutions to be examined far out-number the strength of the staff undertaking the operations.

When e-banking and internet banking are introduced into our banking system, there will be a need for IT audits to be conducted in the areas of organisation and management, system development process, operation and security, communication network, outsourcing process and internal auditing.

Figure 6
Technology-supported Financial Products and Services

No.	Item	Yes/No
1.	Is it conducted regularly ?	-
2.	If not regularly, is it conducted case by case	-
3.	If regularly, objects of audit	-
	Organisation and Management	-
	System development process	-
	Operation	-
	Software and Application, including e – Banking	-
	Security (Authentication, authorisation and protection – including audit trials, encryption)	-
	BCP / DRP	-
	Communication Network	-
	Outsourcing process	Yes
	Internal Auditing	

Source: Survey conducted for this research paper.

5.5 IT-Specialised Supervisors / Auditors

As few banks perform on-line banking services, they conduct their IT audit with IT specialists by applying internal check and management system.

At present, the supervisory staff of the Central Bank lack the technical skills to adapt to the IT implementation. They are in need of international as well as internal training to improve their skills and capabilities in the areas of IT knowledge, IT- related supervision and risk management. The training of the Central Bank staff to upgrade their competence in the field of IT supervision should be an on-going process.

5.6 Coordination among Financial Institution Authorities

Under the guidance of the Banks Supervisory Committee and the Myanmar Banks Association, all banks meet monthly to discuss issues relating to financial matters, compliance with the laws, rules, regulation, etc.

Non-bank financial institutions (NBFIs) are not come under the regulation and supervision of the Central Bank. There is lack of coordination among such institutions.

6. Issues and Challenges

6.1 Issues

The development of Myanmar's banking sector is lagging behind other member countries. There is as yet no specific framework for the implementation and supervision of IT-supported financial products and services. The existing laws, rules and regulations relating to this area do not cover all issues arising from the implementation of e-banking.

The number of qualified IT staff is insufficient and they lack the technical skills to conduct IT supervision. The shortage of supervisory staff is major constraint hindering the implementation of e-banking. The lack of rating agencies is also one of the main limitations.

While financial innovation has led to increased efficiency and convenience to customers, the various associated risks are bound to occur and those risks may be operational risk, credit risk, liquidity risk, legal risk, reputational risk and compliance risk.

6.2 Challenges

Recently, a few banks are providing banking services using on-line system whereas the rest have plans to implement not only on-line services but also IT supported-products and services in the near future. Budget constraint is the major challenge banks face in the innovation of their services and their corresponding need for re-organisation, institutional building and on-going staff training.

Moreover, the enactment of specific law covering IT supervision and formulation of proper policy for the implementation of e-banking are some of the challenges confronting the Central Bank of Myanmar.

7. Policy Recommendations

The relevant authorities have a plan to implement the IT-based financial services gradually to keep abreast with the financial sector development of other member countries. The development of IT infrastructure is ready for implementation of e-banking in the financial sector. The Central Bank needs to liberalise the existing tight restrictions on banks in step- by- step approach.

Top management of banks should be aware of the risks associated with the provision of IT- based financial services and be able to take care of these risks. After the introduction of the supervisory framework, the top management should be thoroughly prepared and equipped to discharge their responsibilities in risk management.

Most of the customers in Myanmar lack IT knowledge. There will be a need for them to be provided some form of training to promote and improve their awareness and knowledge about the different aspects of IT for them to be able to participate in the implementation of e-banking.

For the supervisory staff, appropriate training should be provided for the staff to be thoroughly acquainted with the IT process and the overall supervision in order to equip them to undertake the supervisory tasks.

When e-banking is introduced, the top management of banks should pay attention to the risk management and the supervisory staff should be thoroughly conversant with all aspect of IT supervision as well as the risks management system in the operation of e-banking.

References

William A Barouski and Margaret M. Beutel, "*Supervisory Impact of Technology on South East Asian Banking*", The SEACEN Centre, Kuala Lumpur, Malaysia, May, 1999.

Farid Aulia and Song Ouk-Heon, "*Impact of IT Revolution on the Financial Structure of the SEACEN Countries: Challenges Facing Central Banks"*, the SEACEN Centre, Kuala Lumpur, Malaysia, September 2002.

Basel Committee on Banking Supervision, "*Risk Management Principles for Electronic Banking"*, BIS, July 2003.

Basel Committee on Banking Supervision, "*Management and Supervision of Cross-Border Electronic Banking Activities*", BIS July 2003.

IMF and World Bank, *"Financial Sector Assessment: A Hand Book"* International Monetary Fund and the World Bank, 2005.

Annex 1

Lists of Private Banks' Head Office Branch and Branches in Myanmar as at 29 August, 2008)

Sr. No.	Bank's Name	Head Office Branch	Location of Branches	Total Branches Opened
1	Myanmar Citizens Bank	Yangon	Mandalay	2
2	Co-operative Bank (Public Bank Co., Ltd.)	Yangon	Mingalarzay, Pyinmanar, Aungban, Mandalay(1), Taungngu, Sawbwagyigone, Nyaunglaypin, Wizaya, Bayintnaung,Lanmadaw, Mandalay(2), Mandalay(3), Meikhitla, Bago, Pyi	16
3	Yadanabon Bank	Mandalay	Mandalay (Industrial Zone-1)	2
4	First Private Bank	Yangon	Bayintnaung, Mandalay, Monywa, Theingyizay (C-Block), Pyi, Hinthada, Kyaukpadaung, Magwe, Pakokku, Latha, Myeik, Dawei, Kawthaung, Aungban, Ahlon	16
5	Myawaddy Bank	Yangon	Mandalay, Monywa, Taunggyi, Pharkant, Pathein, Bayintnaung, Kyaukse, Pyinmanar, Myeik	10
6	Yangon City Bank	Yangon	Kyauktada	2
7	Yoma Bank	Yangon	Seingtann, Mandalay (Main), Manmyozay, FMI, Pyi, Magwe, Muse, Lashio, Myaynigone, Bayintnaung, AungLan, Myingyan, Botataung, Yankin, Hlaingtharyar, Kyaukpadaung, Monywa, Pakokku, Kyaukdata, Meikhtila, Latha, Insein, Myitkyina, Mayangone, Mingalarzay, Thingangyun, Myaungmya, Sittwe, Pyinmanar, Kalay, Taungdwingyi, Aungban, Sawbwagyigone, Ahlon, Pathein, Kyaukme, Yadanarbonzay, Pyinoolwin, Kywesekan, Hpaan	41
8	Myanmar Oriental Bank	Yangon	Shwebonthar, Mandalay (1), Lanmadaw, Monywa, Latha, Pyi, Kamayut, Ahlon, Myeik, Tamwe, 35 Street (Mdy), Taung Ngu, Bayintnaung, Pathein, Hinthada, Magwe	17

Sr. No.	Bank's Name	Head Office Branch	Location of Branches	Total Branches Opened
9	Tun Foundation Bank	Yangon	Bayintnaung, Mandalay, Chauk, Yananchaung, Maubin	6
10	Kanbawza Bank	Yangon	Taunggyi, Mingalazay, Mandalay, Lanmadaw, Tarchilate, Bayintnaung, Lashio, Muse, Pakokku, Kawthaung, Myeik, Pazundaung, Pharkant, Maungtaw, Mandalay (2), Mawlamyaing, Hinthada, Myitkyina, Sittwe, Bamaw, Shwegondine, Meikhtila, Magwe, Monywa	25
11	Asian Yangon Bank	Yangon	-	1
12	Myanma Industrial Development Bank	Yangon	Mandalay, Meikhtila	3
13	Myanma Livestock & Fisheries Development Bank	Yangon	Myeik, Muse, Mandalay, Pyapon, Thantwe, Sittwe, Bayintnaung, Maungtaw, Taungkok, Bokalay, Laputta,Mawlamyaing, Kawthaung, Dawei, Kyeemyindine, Aungmingalar, Yuzana Plaza, Hpaan, Shwebonthar, Shwetaungtang	21
14	Sibin Tharyar Yay Bank	Naypyitaw	Yangon	2
15	Innwa Bank	Yangon	Taunggyi, Mineshu, Mandalay, Myitkyina, Monywa, Pharkant, Muse, Lashio, Myaing Kalay, Kamayut, Naypyitaw, Pakokku, Myeik, Sittwe, Loikaw, Kalay, Meikhtila, Myingyan, Pyi, Kung Tung, Dawei, Ann, Magwe, Mawlamyaing, Taungngu, Pathein	27
	Total	**15**	**176**	**191**

Annex 2

Total Asset of the Banking Institutions and the Asset Share

(Kyata in Million)

	2005				2006				2007
	Mar	**June**	**Sept:**	**Dec**	**Mar**	**June**	**Sept:**	**Dec**	**Mar**
Total Assets	5324665	3035059	3180314	3393195	3552867	3745260	4089444	4375357	4580503
CBM	1900015	1989353	2081451	2211769	2388619	2492639	2643373	2813827	3058971
%	35.68	65.55	65.45	65.18	67.23	66.56	64.64	64.31	66.78
MEB	2901616	472580	534618	567471	566653	587516	662924	728710	719331
%	54.50	15.57	16.81	16.72	15.95	15.69	16.21	16.66	15.70
MFTB	-	43915	43812	46502	42611	44291	47838	48827	46805
%	-	1.45	1.38	1.37	1.20	1.18	1.17	1.12	1.02
MICB	25496	30643	34741	33829	33057	34123	38609	37971	36795
%	0.48	1.01	1.09	1.35	0.93	0.91	0.94	0.87	0.80
MADB	19614	33244	41980	45670	25449	52699	56649	61152	35583
%	0.37	1.90	1.32	1.35	0.72	1.41	1.39	1.40	0.78
Private Bank	477833	465304	443626	487868	496392	533906	639967	684786	682933
%	8.97	15.33	13.95	14.38	13.97	14.26	15.65	15.65	14.91

total assets & total loan & capital adequacy

CHAPTER 7

THE SUPERVISORY IMPACT OF TECHNOLOGY ON SEACEN FINANCIAL INSTITUTIONS: ISSUES AND CHALLENGES IN NEPAL

by Shiba Raj Shrestha1

1. Introduction

The Nepalese financial sector comprises mainly the banking and non-banking sector. The Nepal Rastra Bank (NRB) is the central bank and monetary authority of the country. The banking sector consists of commercial banks, while the non-banking sector includes development banks, finance companies, micro-finance development banks, saving and credit co-operatives and financial intermediary non-government organisations (FINGOs) licensed by the NRB. Similarly, the financial institutions such as insurance companies, employees' provident fund, citizen investment trust, deposit insurance and credit guarantee corporation, postal saving banks and the Nepal Stock Exchange (NEPSE) can be treated as non-banking institutions. Apart from these, the informal financial system also persists in many rural areas.

The banks and financial Institutions (BFIs) in Nepal are rapidly increasing their use of technology to streamline operations, expand trading activities, improve service and minimise information risks. In a similar fashion, the financial landscape in the SEACEN countries has also been rapidly developing in breadth and depth to meet this challenge. The development of financial markets requires new products, new players and internationally practiced rules with a robust financial infrastructure that ensures efficient, secure and timely clearing, settlement and payment of financial transactions. Information Technology (IT) has been a major contributor to the promotion of financial markets in Nepal by performing a dual role as an engine of development of financial products and as an enabler of the operation of financial institutions.

IT has created the global market by linking local markets through networks. The use of IT has flattened the business hierarchy by lessening inefficient layers and enabled the BFIs to reach the consumer directly. Remarkably, most conservative BFIs in recent times have started to move forward to satisfy customers' demand through the use of IT in Nepal.

---

1 Author is Director, Financial Institution Supervision Department of Nepal Rastra Bank.

Many BFIs in Nepal are making huge investments in IT to maintain and upgrade their infrastructure, not only to provide new electronic information-based services, but also to manage risk positions and pricing. The on-line retail banking has made it possible for the smaller financial institutions to take advantage of new technology at affordable costs. These developments may ultimately change the competitive landscape in the financial services in Nepal.

IT is also changing the supervisory and regulatory landscape in Nepal. It is creating new tools for supervisors to cope with the supervisory challenges. Technology-driven issues such as privacy and the nature of electronic communications have reached the forefront of the policy agenda. The Cyber Law and Electronic Transaction Act of Nepal do not cover all the issues pertaining to IT-related banking activities. The regulations and guidelines for e-banking and risk management affiliated to the same are yet to be developed in Nepal. To date, the NRB has not formulated any regulatory and supervisory framework pertaining to the use of IT by the Nepalese BFIs in their operation and service delivery. However, while supervising the application of IT in the BFIs, the NRB is following the 14 principles of risk management for electronic banking issued by the Bank for International Settlement (BIS).

The main objective of this paper is to assess the implementation of IT in the BFIs' operations and service delivery. This paper highlights the BFI's financial risks in association with the use of IT in the payment and settlement systems. This paper also focuses on the experience of Nepal and the lessons learned concerning the supervisory impact of technology and recommends policy prescriptions. Moreover, this paper would also be a part of the SEACEN research project on "The Supervisory Impact of Technology on SEACEN Financial Institutions: Issues and Challenges" and could be used for further study.

This paper is organised in seven Sections, as follows.

Section1 outlines the background, motivation and objectives of the paper and presents a brief overview of the paper.

Section 2 provides a brief overview of the Nepalese economy, banking and financial system.

Section 3 surveys the IT implementation and dwells mainly on the development of the technology infrastructure, national payment system, presence of technology-supported financial products and services.

Section 4 focuses on the impact of IT implementation on the BFIs and assesses the general operational risk faced by the BFIs with regard to the technology-supported financial products.

Section 5 takes an overall look through the prevailing IT supervisory framework and regulations.

Section 6 addresses the issues and challenges faced by the country with regard to the implementation, regulation and supervision of the application of IT in the financial sector.

Section 7 presents the conclusion and a summary of the recommendations.

The relevant illustrative appendices have been attached to the paper. It is expected that this paper would prove useful to the policy makers of the NRB, SEACEN Centre, SEACEN member countries and other concerned authorities.

2. Overview of the Financial System

2.1 Brief Introduction of the Nepalese Financial System

The financial sector of Nepal has evolved rapidly over the past two and half decades following the government's liberalisation policy. Almost all kinds of financial markets, viz. money market, capital market and insurance business have witnessed growth. The financial sector is the only sector that is buoyant and growing when almost all other sectors of the economy went through troubled times over the last one and half decade when the country's law and order situation deteriorated.

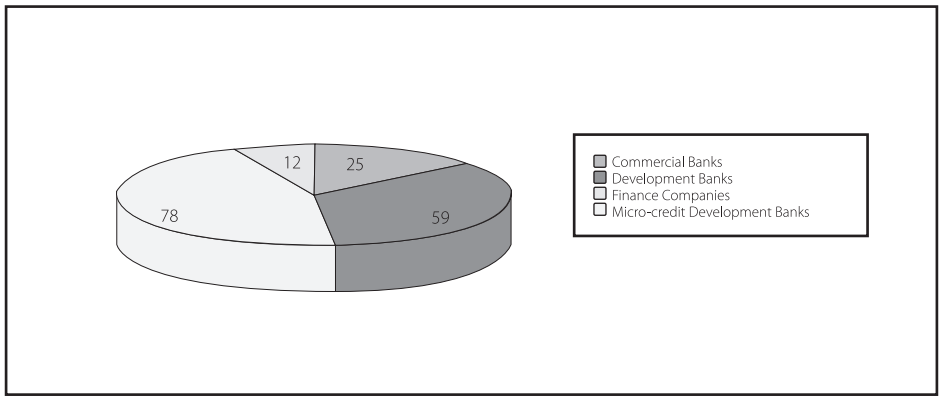
The Nepalese financial system can be divided into four groups: bank and financial institutions (BFIs) regulated by Nepal Rastra Bank (the central bank of Nepal), insurance companies regulated by the Insurance Board, the Nepal Stock Exchange (NEPSE) regulated by the Securities Board of Nepal (SEBON) and the other non-bank financial institutions, like the Employees' Provident Fund, Citizen Investment Trust, Deposit Insurance and Credit Guarantee Corporation, regulated by the Government of Nepal (GoN). Besides, around 3392 saving and credit cooperatives are licensed by the Cooperative Department. The involvement of the informal sector in the system particularly in the rural areas is also present.

The banking and financial market is functioning in compliance with the legal enactments and provisions like the Nepal Rastra Bank Act 2002, the Bank and Financial Institution Act (BAFIA) 2006, the BFI Debt Recovery Act 2002, the Financial Intermediation Act 2002, the Company Act 2006, the Secured Transaction Act 2006, the Unified Directives 2005 issued by NRB, etc., and the other circulars which are issued from time to time.

2.2 Number of BFIs and Branches

Focusing mainly on the BFIs, there are 25 commercial banks, 59 development banks, 78 finance companies, 12 micro-finance development banks, categorised as "A", "B", "C" and "D" respectively. Apart from these, there are 16 saving and credit co-operatives and 46 Non-government Organisations (NGOs) licensed for limited banking activities. Hence, the total number of the BFIs licensed, regulated and supervised by NRB is 236.

Figure 1
Number of Banks and Financial Institutions in Nepal



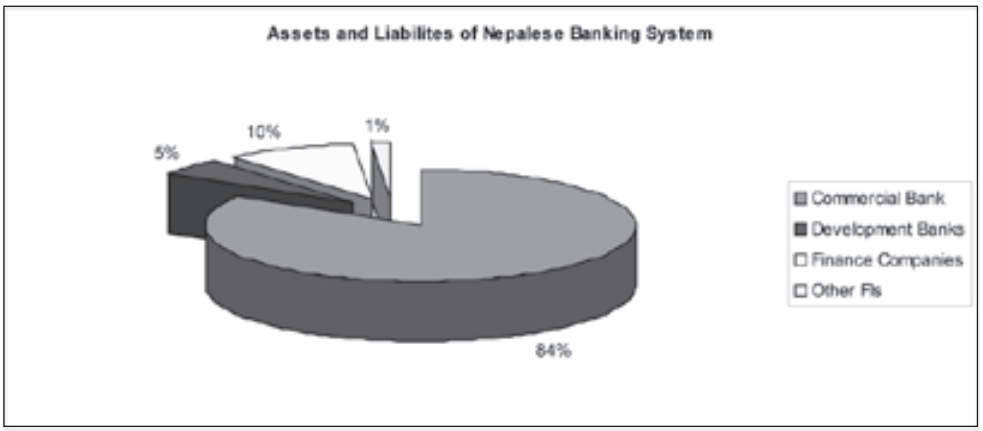
Type	Number of BFIs (in mid-July)								
	1980	**1985**	**1990**	**1995**	**2000**	**2005**	**2006**	**2007**	**2008**
Commercial Banks (A)	2	3	5	10	13	17	18	20	25
Development Banks (B)	2	2	2	3	7	26	28	38	59
Finance Companies(C)	-	-	-	21	45	60	70	74	78
Micro Credit Development Banks (D)	-	-	-	4	7	11	11	12	12
Saving and Credit Cooperatives	-	-	-	6	19	20	19	17	16
NGOs (Limited Banking Activities)	-	-	-	-	7	47	47	47	46
Total	**4**	**5**	**7**	**44**	**98**	**181**	**193**	**208**	**236**

The number of commercial bank branches operating in the country has reached 574 in mid-August 2008. Of the total bank branches more than 46.34%, i.e., 267 bank branches are concentrated in the central region. Meanwhile, 113, 117, 46 and 31 bank branches are operated in the eastern, western, mid-western and far-western region, respectively. Likewise, the number of branches of development banks and finance companies operating in the country has been reached 120 and 145, respectively, in mid-August 2008.

2.3 Total Assets of the Banking System

The total assets/liabilities of the Nepalese banking system is recorded at Rs. 678,516 million (Commercial Banks Rs. 566,412, Development Banks Rs. 36,905, Finance Companies Rs. 65,720 and rest from the other financial institutions) in mid-August 2008. The banking sector, being the largest financial sector, alone held more than 80% of the total assets/liabilities of the financial system. As of mid-August 2008, the commercial banks occupied 84% of the total assets/liabilities of the financial system; finance companies 10%; development banks 5%; and micro-credit development bank and others 1% .

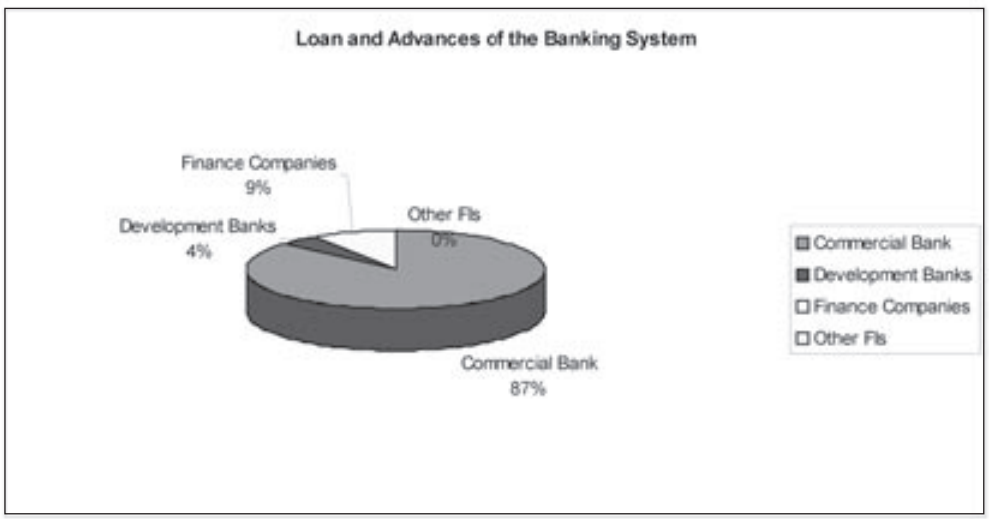
Figure 2
Assets and Liabilities of the Nepalese Banking System



2.4 Loans and Advances of the Banking System

The loans and advances reported substantial growth of 19.31% in mid-August 2008 compared to 14.42% in the same period of last year. In mid-August 2008, the total loans and advances reached to Rs. 498,361 million (Commercial Banks Rs. 431,332 million, Development Banks Rs. 21,757 million, Finance Companies Rs. 44,659 million and rest from other financial institutions). During the period from 2001 to 2008, the annual average growth rate of loans and advances was recorded at 15.45%. The higher growth rate of loans and advances compared to deposit mobilisation was attributed to the increase in the credit deposit ratio of financial system to 78.78% in mid-August 2008, up from 74.55% in the mid-August 2007.

Figure 3
Loans and Advances of the Banking System



2.5 Capital Adequacy of the Banking System

In Nepal, the capital adequacy ratio (CAR) to be maintained by the BFIs has remained at 11% and the core capital ratio at 5.5% of the risk-weighted assets. Since mid-July 2008 the commercial banks are required to follow the new capital adequacy requirements based on BASEL II and they are to maintain 6% core capital ratio and 10% capital fund of the risk-weighted assets. The capital fund of commercial banks compared to the risk-weighted assets remains negative till mid-July 2007, and recorded positive at 4.04% (Rs. 154,603 million) in mid-July 2008.

2.6 Non-performing Loans of the Banking System

The proportion of the non-performing loans (NPL) to the total gross loans of commercial banks was recorded at 8.94%; of development banks at 4.50%; and of finance companies at 4.39% in mid-August 2008.

2.7 Capital Market Activities

The year on year NEPSE index increased by 53.7% to 1084.76 points in mid-August 2008. The market capitalisation increased to Rs. 423.7 billion in mid-August 2008. The market capitalisation to the GDP ratio is estimated to be 44.8% up from 23.5% a year ago. The monthly turnover to market capitalisation ratio remained at 0.70% in mid-August 2008 as compared to 0.89% a year ago.

The weighted average monthly 91 days Treasury Bills rate reached to 5.17% in mid-August 2008. The weighted average monthly interbank rate rose to 5.15% in mid-August 2008 from 4.1% a year ago.

2.8 IT-supported Financial Products Statistics

In Nepal, 24-hour ATM service facilities are available from approximately 180 ATM outlets throughout the country in the major cities serving around 700,000 cardholders. The customers of the BFIs can use VISA/MASTER/SCT cards at any ATM machine for cash withdrawals, account transfers, bills payment, balance inquiries, etc.

3. Survey on IT Implementation

3.1 Presence of Technology-supported Financial Products and Services in Nepal

IT can be defined as the use of computers to acquire, store, process and distribute information. The use of IT in banking is pervasive and indispensable. Nowadays, data is stored in electronic databases. Few banks can quickly provide detailed information on deposit and other accounts when their IT system is down. Competitive pressures and the availability of technological solutions have forced the BFIs to be highly dependent on IT. Most banking organisations now have IT departments responsible for the design, administration and maintenance of computer systems and the technological infrastructure.

With the advancement of IT, business organisations are increasingly dependent on computerised information system to carry out their operations, process, maintain and report essential information. The use of IT has revolutionised the banking and financial sector in Nepal. The manner in which the banks and the BFIs are offering the financial services is undergoing a radical change.

A wide array of new financial services such as Electronic Banking, Tele-banking, Electronic Funds Transfer, Electronic Money, Smart Cards, Debit Cards, and Credit Cards are fast gaining ground. Now, the Nepalese BFIs are aware of the rapid changes in IT and its implication for the business environment. It is critical for all the BFIs to provide customers with convenient financial services quickly and reasonably. The BFIs have been progressively utilising IT and have undergone dramatic advances in recent years. The BFIs, in offering their banking products, have increasingly capitalised on the use of the Internet and mobile phone. Following are the main channels that are available for service delivery in the Nepalese financial sector:

- Automated Teller Machines (ATM)
- Credit Cards
- Debit Cards
- Point of Sales (PoS)
- Internet Banking
- SMS Banking
- Any-branch Banking (ABB)

3.2 Types of Banking Software and Service Providers in Nepal

There is heterogeneity of software used by the BFIs in the Nepalese financial system. Most of the commercial banks have used foreign software supplied by

Indian Companies whereas the other BFIs have used domestic software. The variety of software available in Nepal can be seen below:

3.2.1 Commercial Banks

- Pumori Plus (Mercantile Office System, Nepal)
- Finacle (Indian Supplier)
- Globus (Indian Supplier)
- Newton (Indian Supplier)
- Flexcube (Indian Supplier)

3.2.2 Development Banks

- Pumori Plus (Mercantile Office System, Nepal)
- Bank Plus (PCS, Nepal)

3.2.3 Finance Companies

- Microbanker (FAO Microbanking System)
- Bank Plus (PCS, Nepal)
- Pumori Plus (Mercantile Office System, Nepal)
- Proban (Progression IT Solution, Nepal)
- FinAcct (FASS, Nepal)
- FoxPro Based Local Software (Subpack Consult, Nepal)
- FINMIS (Mandala Software Pvt. Ltd., Nepal)
- FINMAN (N. K. Joshi and Company)

3.2.4 Debit/Credit Card Service Providers

- Smart Choice Technology/SCT, Nepal (No. of Card Users - 500,000)
- Visa Electron International (No. of Card Users - 200,000)

3.2.5 Network Infrastructure Providers

- Nepal Telecom
- Subisu Cablenet
- Worldlink Communications
- Banks Own VSATs
- Other Service Providers

3.3 Computerised Banking System

Technological innovation has significantly impacted the financial sector of Nepal. The past few years have seen a truly phenomenal pace of new technology adoption among even the most conservative banking organisations. All the banking organisations have adopted automated core banking systems. By their investments in IT, organisations are not only anticipating reductions in operating costs through efficiencies gained from the streamlining of back-office processing and the elimination of error-prone manual input of data. They see opportunities

in enhancing the convenience and value of the existing products and services to their current customers and in attracting new customers by offering new products and services The Nepalese BFIs have started utilising the recent innovations in IT, such as the Internet and mobile communication.

3.4 SMS and Internet Banking

Internet banking currently used by the Nepalese BFIs can be classified into two categories, informational and transactional. The informational website provides banking information including products, services, interest rates, foreign exchange rates, 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. Most of the BFIs are using informational website only. The BFIs which are using transactional websites are limited to intra-bank fund transfer from one account to another account of the same customer. They are also providing utility bill payments facility.

SMS banking, which is becoming popular these days, provides information to customers' cell phone. They provide customer balance inquiry, mini statement, transaction information, foreign exchange information, etc. Most of the BFIs in Nepal have already started the services based on the Internet and SMS.

3.5 Debit/Credit Card and ATM

All the private commercial banks, a public bank and a few development banks and finance companies have issued debit cards to their customers and have provided their customers with facilities to view their account balance and withdraw cash from the ATM machine. All the commercial banks have issued debit and credit cards. The total number of cardholders has reached approximately 700,000. To date, 180 ATM machines have been installed in the urban centres of the country. The service providers are Smart Choice Technology, Nepal (500,000 card users) and Visa Electron International (200,000 card users). The network of ATMs has been expanded to cover almost all the main cities outside the Kathmandu valley. The shared network of ATMs is also connected to a network in India with more than 50,000 machines. Most of the BFIs have shared ATM networks enabling the customers to access their account from machines other than their own BFI. There are some 5,000 Point of Sale (POS) machines enabling customers to purchase commodities in a number of departmental stores.

3.6 Business Continuity Planning

Business continuity planning (BCP) includes policies, standards and procedures for ensuring that specified operations can be maintained or recovered in a timely fashion in the event of a disruption. Business continuity planning is about

maintaining, resuming and recovering business operations - not just the recovery of the information system whereas a disaster recovery plan deals with recovering IT assets after a disastrous interruption. It is essential to minimise the operational, financial, legal, reputation and other material consequences arising from a disruption. Since every organisation is always at risk due to natural calamities, electricity breakdown, environmental disaster, cyber and hacker activities, etc, it is critically essential for every BFI to develop a BCP. All the commercial banks do have proper business continuity planning. However, very few development banks and finance companies have proper business continuity planning.

3.7 Information Technology and Security Policy

While the use of IT provides a key competitive advantage to the BFIs, it can also jeopardise the success and sustainability of a BFI if it is not properly implemented, monitored, and controlled. Since business activities require information to meet business objectives, IT must be designed and aligned with business and corporate objectives to enable a BFI to take full advantage of its information for it to maximise benefits, capitalise on opportunities and gain a competitive advantage. To ensure this, the BFI should have an IT policy accommodating all the critical IT activities. It is also vital for each BFI to have a sound information security policy for managing risk systematically throughout the BFI in line with each situation, under the active involvement of management. A significant number of BFIs in Nepal lack IT and Information Security (IS) Policy, which is impeding the capability of the BFIs to take full advantage of its information. These BFIs may not be optimising their business performance with regard to maximising benefits, capitalising on opportunities and gaining a competitive advantage. Few BFIs, which possess the policy, also do not have separate IT Security Policy.

3.8 Outsourcing

Outsourcing refers to the sub-contracting of IT activities to external organisations that are normally run by the organisation itself. The outsourcing function ranges from a help desk; a project completion; maintenance of equipment and full IS function. With the advent of rapid changes in technology and competition, the BFIs tend to reduce costs and improve their services by outsourcing some technology-related functions to third parties. The full scope of outsourcing encompassing entire IT resources and operations, including location, equipment, hardware, software, staff, facilities, communication and other necessities to the third-party service providers, has not yet been practiced by the Nepalese BFIs. Partial outsourcing in which a BFI may acquire a certain service of a provider, for example, maintenance of computer hardware, formulation of policies and procedures, network communication media, etc., is in practice in most of the BFIs in Nepal.

3.9 Development of Technology Infrastructure and the National Payment System

Telephone, cell phone, Internet, fiber optic and satellite communications are the common means of tele-communication in Nepal. The Nepal Telecom, Subisu Cablenet and Worldlink Communications are the major service providers for the communication infrastructure in Nepal. The commercial banks also have their own VSATs for their communication network. Internet and cell phone have become increasingly popular among the economically active population, but the service is not so widespread. Access to the Internet in Nepal is available in a variety of modes - dial-up facility, cable connection, satellite and wireless connection.

The transmission networks in Nepal consist of backbone link, microwave radio network and optical fiber network, though most of them suffer from the lack of capacity. Satellite network is in operation in the Himalayan region, where it is difficult to lay wire line network. For the microwave radio network, most of the systems deployed are of the asynchronous type and in operation as trunk and branch networks. However, several SDH Microwave systems are in use in some nodes. Currently, a microwave radio link between Nepal and Bangladesh has been set up.

With regard to the optical fiber network, there are a ring-shaped 2.5 Gbps optical fiber network in the Kathmandu Valley and a SDH Optical Link along the East-West Highway. Also, an optical fiber network between Nepal and India is in operation. For the access links, WLL and mobile network have been used. ADSL service has started recently.

For satellite network, earth stations, RSAT and VSAT are in use and the deployment of the DSAT system has been planned. Network coverage and Internet access is rapidly increasing.

Four universities and affiliated colleges are providing ICT education courses. The distribution of ICT workforce has been heavily skewed in Kathmandu valley where 69% of ICT workforce is concentrated.

The Government of Nepal (GoN) has initiated a comprehensive strategy on rural development to promote balanced development of the ICT industry around the country, which is currently disproportionately concentrated in Kathmandu valley.

The national payment system is the backbone for the economic development of the country, which supports non-cash payments in the country. All commercial banks and a few development banks and finance companies have joined a common Payment Network through Smart Choice Technology and Visa Electron to support the payment of debit card and credit card, fund transfer and remittance services. The domestic remittance and fund transfer services are also provided by Nepalese BFIs. Most of the commercial banks and private companies, like International Money Express (IME), Prabhu Money Transfer, provide international fund transfer and remittance services with their own network and also with joint collaboration with the Western Union Money Transfer, Money Gram, and some other international BFIs.

The Nepalese financial system lacks real time gross settlement (RTGS) in its payment system. The cheque clearing system is provided by the NRB for its member BFIs. The NRB in coordination with Ministry of Finance provides government security settlement services. Nepal is without a scripless security settlement system. The national payment system in Nepal is not so savy and sophisticated as compared to the payment systems of other developed Asian countries. A lot of effort is required to boost up the national payment system in Nepal.

Significantly, the increasing development and expansion in the field of networks, Internet and ICT workforce indicate that Nepalese BFIs are able to capitalise on the use of IT in their financial activities. However, there is absence of strong support from the Government particularly in the implementation and development of IT-related policies. The utilisation of IT in the Nepalese financial system is being constrained by the following major infrastructure and technology issues:

- Poor telecommunication infrastructure characterised by slow Internet connectivity, costly and unreliable connections.
- Limited e-security knowledgeable resources in the country.
- Lack of certification authority and public key infrastructure (PKI).
- Lack of automated payment system.

Though Nepal has a lot of work to do in the development of a national payment system and communication infrastructure, the existing communication infrastructure is gradually supporting the potential development of IT in the BFIs in the overall development of the Nepalese banking system. With this background, the status of the installed IT infrastructure in Nepal is shown in the following table.

Figure 4
Status of Installed IT Infrastructure

No.	Item	Yes/No
1	Communication Network	
	Cable (Phone line)	Yes
	Satellite	Yes
	Fiber Optic	Yes
2	Use of Cellular Phone	Yes
	Is it relatively wide spread?	No
3	Use of Internet	Yes
	Is it relatively wide spread?	No
4	National Payment System	Yes
	Operated by government agency / central bank	Yes
	Operated by an independent or private company	No
5	Automated/Computerised Payment System	No
6	RTGS	No
7	National Securities Settlement System	Yes
	Operated by government agency / central bank	Yes
	Automated/Computerised Settlement System	No

3.10 Presence of Technology-supported Financial Products and Services

Most of the IT-related financial products prevailing in the global market are also available through the Nepalese BFIs. The following IT-related products are offered in the Nepalese banking system.

Figure 5
IT-related Products

No.	Item	Yes/No
1.	Credit Card	Yes
	National (only used in the country)	Yes
	International	Yes
2.	Debit Card	Yes
	National (only used in the country)	Yes
	International	Yes
3.	ATM	Yes
	Individual bank	Yes

	Nationally-shared ATM	Yes
	Internationally-shared ATM	Yes
4.	Electronic Fund Transfer (EFT)	Yes
5.	EFT at Point of Sale	Yes
	National (only within the country)	Yes
	International	Yes
6.	Remittance Service	Yes
	Domestic companies	Yes
	International companies	Yes
7.	Phone Banking	Yes
	Informational	Yes
	Transactional intra bank	Yes
	Transactional inter bank	No
8.	Mobile/SMS Banking	Yes
	Informational	Yes
	Transactional intra bank	No
	Transactional inter bank	No
9.	Internet Banking	Yes
	Informational	Yes
	Transactional intra bank	Yes
	Transactional inter bank	No
10.	Pre-paid card	Yes

3.11 The Heterogeneity/Homogeneity of the Technology Implemented in the Financial Institutions

Most of the BFIs in Nepal have computerised their operations and are providing various IT-related services to their clients. Following the common trend in the global financial market, the Nepalese BFIs are using a variety of software and technology for their core banking operations. The BFIs use different platforms to implement their IT software with different security and risk management policies and working procedures. Due to the high maintenance cost and budget constraint, most of the BFIs in Nepal are using heterogeneous and less-sophisticated domestic software for their banking operations. Finance companies in particular are using diverse software systems developed by local vendors, systems whose thorough verification has not been ensured. The heterogeneity of the IT systems implemented by the Nepalese BFIs sometimes creates hang-up problem and does not provide the desired information and reporting. Moreover, the IT expert of the supervision team is faced with the various implementation modalities in the software and hardware, which require diversified knowledge and higher level of

skills. However, experienced and highly skilled IT supervisors are not available in the Nepal Rastra Bank. The outsourcing of IT experts is expensive and they are sometimes not available for the performance of the desired service. Keeping this in view, the status of IT-related applications in addition to IT-related products is given below.

Figure 6
Status of IT-related Applications in Addition to IT-related Products

No.	Item	Status
1.	Core Banking: General Ledger, Third Party Fund, Loan and Consumer Information File	Yes
2.	Treasury	Yes
3.	Remittance	Yes
4.	Trade Finance	Yes
5.	Corporate Online Service	Yes

4. Impact of IT Implementation on Financial Institutions

4.1 Assessment of the Operational Risk of BFIs with regard to the Technology-Supported Financial Products and Financial Institution Operation

The use of IT has become inevitable for the Nepalese BFIs. The proper implementation of IT confers various and significant opportunities like improved service delivery, enhanced efficiency, market penetration, competitive advantage, better profits and value maximisation. As such, the Nepalese BFIs are rapidly increasing their use of technology to streamline operations, expand trading activities, improve service and minimise risks. Technology has increased the size of data and information being processed, resulting in a significant impact on the control environment in the Nepalese banking system. Due to the BFIs' high dependence on IT, continuous watch on their information system should be given prime importance by the BFIs to safeguard their information assets and the financial system.

Supervisors are concerned about the operational and systemic risk, within which IT and security risks are prominent. The importance of IT in the BFIs requires supervisors to assess how well IT resources are managed and how effectively IT risks are controlled by the BFIs. Some BFIs have their own IT department or operational risk department with specialists in this field. These teams can carry out focused IT inspections. There are also jurisdictions for which senior management and the supervisors rely on external auditors for the assessment of IT risks.

Typically, the dynamic and sophisticated banking products and services will attract economically active people. To retain customers, BFIs find it mandatory to have the latest technology implemented in their operations. However, the use of technology in banking activities also brings about various risks. Thus, the BFI board and senior management should always review each of the processes to adapt and expand the BFI's risk management practices as necessary to address and mitigate the risks posed by IT-related banking activities. Considering the types of software used by the Nepalese BFIs and their services, the attendant risk factors have to be assessed, monitored, controlled and managed for better IT implementation in the Nepalese banking system.

4.2 Strategic Risk

Strategic risk refers to the risk of IT operations potentially affecting a BFI's ability to achieve its strategic objectives. For example, the decisions to delay or forego essential enhancements to a bank's IT infrastructure could result in a strategic business activity not achieving profitability or market-share objectives.

4.3 Operational Risk

Operational risk is the primary risk associated with IT. It can arise from several areas including back-office operations, transaction processing and systems development. Threats to IT resources can be internal or external and can result in disruptions to banking services and can effect critical banking operations.

4.4 Liquidity Risk

Liquidity risk occurs due to the heavy withdrawal of funds at any time of the day due to adverse information about the BFI.

4.5 Credit Risk

Credit risk is the risk that arises from the difficulty in authenticating the identity and creditworthiness of a client due to geographical distance.

4.6 Reputational Risk

Reputational risk is the risk of damage to a BFI, for example, due to the failure of its IT to maintain the confidentiality of customer information. Reputational damage to a BFI, which could also result from a breakdown in IT that becomes public knowledge, can result in liquidity, profitability and capital adequacy problems.

4.7 Legal Risk

Legal risk is the risk of loss from legal actions or proceedings involving IT products and services.

4.8 Compliance Risk

Compliance risk arises due to the possibility that the IT implementation is not in compliance with the prevailing rules and regulations. For example, violation of customers' information agreement, wrong mechanism of transaction.

The NRB has not prescribed any specific risk management guideline for the Nepalese BFIs. Some of the commercial banks have developed their own risk management modality for IT-based operation. However, most of the Nepalese BFIs are lagging behind in their risk management system. The following types of risk are encountered in the Nepalese financial system from the use of IT as a channel for service delivery.

Figure 7
Types of Risks

No.	Item	Yes/No
1	Operation Risk	**Yes**
2	Liquidity Risk	**Yes**
3	Credit Risk	**Yes**
4	Strategic Risk	**Yes**
5	Reputation Risk	**Yes**
6	Legal Risk	**Yes**
7	Compliance Risk	**Yes**

4.9 Risks and Impact of the Use of IT in Financial Products and Financial Institution Operation to the Supervisory Practices

IT-related banking products have unique characteristics that may increase the BFI's overall risk profile and the level of risks associated with the traditional financial services, particularly strategic, operational, liquidity, credit, legal and reputation risks. These unique characteristics of IT-related banking products and services include:

- Pace of technological change and cost of modification and replacement,
- Changing customer expectations and cost of product enhancement,
- Increased visibility of publicly accessible networks (e.g., the Internet) and potential cyber crime,

- Less face-to-face interaction with BFI customers and social engineering,
- Need to integrate e-banking with the BFIs' legacy computer systems and cost of integration compared to revenue generation,
- Dependence on third parties for necessary technical expertise and cost of outsourcing,
- Proliferation of threats and vulnerabilities in publicly accessible networks and cost of hacking and cracking information, and
- Technology failure and cost of downtime and error.

4.10 Prevailing Technology Supervisory Framework and Regulations in Nepal

The Electronic Transaction Act, 2061 provides the legal provisions for authentication and regularisation of the recognition, validity, integrity and reliability of generation, production, processing, storage, communication and transmission system of electronic records by making the transactions to be carried out by means of electronic data exchange or by any other means of electronic communications, reliable and secured. However, to date there is no regulatory framework for electronic banking. In view of the introduction of electronic banking in the Nepalese BFIs and the maximum use of IT in the banking sector, it is imperative to establish a regulatory framework to ensure the safety of depositors' money. The Cyber Law and Electronic Transaction Act of Nepal do not cover all the issues and lack effective implementation. The regulations concerning e-banking and the guidelines for e-banking risk management have not yet to be developed. Likewise, there is no specific supervisory framework and regulations for IT supervision in Nepal. The NRB also has not issued any regulation on this matter. However, while conducting supervision of the BFIs, the primary functions of IT supervision would be to evaluate the system's efficacy and security protocols, in particular, to evaluate the BFI's ability to protect its information assets and properly dispense information to authorised parties.

4.11 Scope of IT Supervision

The scope of the NRB's supervision of IT-related banking operations, includes data, application systems, technology, facilities and people. The following are the supervisory areas of the NRB:

4.11.1 Information Security and Control Measure

The connection of the information system to the open network exposes it to unknown sources globally and increases the possibility of fraud, hacking, cracking, etc. Accordingly, the use of IT poses a risk to the business, and hence is the concern of supervision. Adequate physical and logical access controls are important since they can protect data, system and resources from unauthorised persons.

i. Physical Security

This is about the control of environmental exposure, including fire, flood, lightning, equipment failure, along with the human factor like riot, terrorist, etc. The lack of physical security may lead to unauthorised access to equipment and data.

ii. Logical Security

It comprises data, system and network access control. The lack of adequate logical security may result in technical exposure to unauthorised implementation or modification of data and program at the network, platform and database or application level. A BFI 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 the Internet does not require face-to face contact, non-repudiation becomes another major issue as the ability to prove that a customer did request a transaction on service. Therefore, security and control measures are always a prime concern of supervision.

4.11.2 IT Outsourcing

Outsourcing is carried out with a third-party service provider residing domestically or abroad. Since BFIs' data including customer and transaction data are processed by other parties, a BFI must safeguard its data integrity, security and confidentiality to prevent data leakage and mishandling. Though operated elsewhere, system reliability and availability still fall under the BFIs' responsibilities. All of these issues can in fact impact the BFIs' reputation, image and credibility.

4.11.3 Policy Perspective

To reap the benefits of IT and the return on investment, IT should be aligned with the organisation and the BFIs must have comprehensive IT policy and procedures in place. To ensure the sound development of the financial services sector, while reaping the benefits from the remarkable advancement of the IT revolution, organisations should implement IT guided by proper policy. The BFIs should have strategic plans and policies emcompassing every IT activity, including security, contingency, outsourcing, human resource, etc. It is ultimately the responsibility of management and the board to ensure that the IT resources are utilised to the full extent.

4.11.4 System Availability

This includes the BFIs' readability for being able to run the business without any disruption in case of all kinds of disaster. The inability of organisation to start the business activity smoothly in case of disruption may result in the loss of not only the reputation of the organisation, but in the confidence of customers in the electronic delivery channel. To ensure the system availability, the organisation must periodically test its business continuity plan.

4.11.5 Data Integrity

To ensure the reliability and completeness of system functionality and to verify that the data is processed in an accurate and timely manner, it is critical for the BFIs to have sound application controls in place. In this regard, they should have controls built in the procedure and programmed into the system to ensure the integrity of input, process and output. Data and system integrity can reflect the effectiveness of system development, acquisition and change-control procedure. The control can be either technical or manual, or both. The 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. Finally, a BFI should provide alternative resources for backup and recovery and ensure that they can be available during the event of a disruption.

4.12 Strength and Weaknesses of the Supervisory Procedure in Nepal

IT can play a very significant role in the efficient delivery of the central banking functions whether it is maintaining price stability or safeguarding the integrity of the financial system, improving payment and settlement functions, currency management function or providing better clearing and payment service, monitoring the effectiveness of monetary policy initiatives or conducting effective open-market operation. Being a monetary authority, the NRB has to closely monitor the progress of IT, among other things, as it may effect the implementation of monetary policy in various ways, like for instance IT-induced changes to the payment and settlement systems and the impact of IT on day-to-day market operations, etc. Similarly, being a regulator and supervisor of the banking and financial system, the NRB has to be fully aware of the IT infrastructure being used by the BFIs in order to maintain financial stability as adoption of new technology may give rise to risks in the system.

Like in other SEACEN countries, the Nepalese BFIs are operating with high operational and systemic risk. Many BFIs in Nepal are introducing IT-related products without adequate risk assessment, planning and cost-benefit analysis. Most of the BFIs in Nepal lack comprehensive security policy to minimise the various IT-related risks. The concept of IT audit has not been practiced in most of the Nepalese BFIs. The NRB as a regulatory and supervisory body has not formulated any policies, procedures, guidelines and directives for the regulation and supervision of electronic banking transactions and for the monitoring of how well IT resources are managed and how effectively IT risks are controlled by BFIs. The supervision of the BFIs, especially for IT-based transactions, is being conducted on an ad-hoc basis based on the personal judgement of the IT supervisors. Thus, it is most urgent for the NRB to formulate an appropriate regulatory and supervisory framework for IT implementation to facilitate the development of a resilient banking system. The NRB is endeavoring to develop a proper regulatory and supervisory framework for IT-based banking transactions in consultation and discussion with the all stakeholders. When such a framework is in place, it will be easier for the NRB to conduct standardised IT supervision uniformly and systematically. The NRB supervisory framework would also make it the responsibility of the the board and senior management of the BFIs for identifying, managing and monitoring the risks in the implementation IT. The NRB supervisory framework would also ensure that the BFI's IT implementation procedures are in compliance with all the prevailing regulations and the risks are assessed in a proper and timely manner.

About the NRB, it introduced a mini-computer in 1982 to process data of the Second Family Budget Survey. The systematic computerisation process in the NRB started only in 1992 with the establishment of the Computer Division, which was later upgraded to a separate department, i.e., Information Technology Department. The departmentis is involved in building new software applications, supporting already built applications, maintaining the Local Area Network (LAN), Internet/ Intranet, addressing connectivity issues between NRB district offices and central office, designing and periodically updating NRB's official website and reviewing and improving IT systems of the NRB. However, the pace in upgrading the system in the NRB is very slow. As a result, the NRB has not been able to reap the full benefits of IT even after a continuous effort of more than a decade. Since the information and communication technology (ICT) is instrumental in contributing to the achievement of corporate objectives, the IT department of NRB is engaged in formulating the ICT strategy of NRB. Accordingly, the following are the three broad ICT strategies proposed for implementation:

- Formulate and implement ICT policy.
- Enhance IT capacity.
- Gradual transformation of workflow towards paperless environment.

5. Prevailing IT Supervisory Framework and Regulations

5.1 Principles of Supervisory Framework and Regulations

The regulation and supervision of the financial and banking system purposes to develop a secure, healthy and efficient payment system, maintain the stability and healthy development of the banking and financial system, and enhance public credibility towards the entire banking and financial system of Nepal, The primary functions of IT supervision are to evaluate the system's efficacy and security protocols and the BFI's ability to protect its information assets and properly dispense information to authorised parties. While conducting the supervison of the BFIs, the Bank Supervision Department (BSD) and the Financial Institution Supervision Department (FISD) appoint one IT expert in the supervision team. However, the IT supervision has been remained inactive and ineffective due to the lack of specific supervisory framework, regulations and adequate expertise. The IT supervision is conducted alongside the normal supervision with the inclusion of an IT expert in the supervision team. The IT supervision is solely based on the personal judgement of IT supervisor. However, attempt has been made to conduct the supervision based on the frame of reference provided by the 14 BIS principles of risk management on electronic banking.

It is urgent for the NRB to formulate a scientific and dynamic IT supervisory framework that is needed to protect the interest of depositors, enhance market competition, develop the banking system, establish risk-based management system, and ensure regulatory compliance, However, it may take a few years to develop a concrete IT supervisory framework for the Nepalese banking system. In the absence of an IT supervisory framework, the NRB supervisors are following the 14 principles of risk management for electronic banking issued by the Bank for International Settlement (BIS). The principles are grouped under the three board categories presented below. However, these principles are not weighted by order of preference or importance.

5.2 Board and Management Oversight (Principles 1 to 3)

1. *Effective management oversight of e-banking activities.*
   The board of directors and senior management should establish effective management oversight over the risks associated with e-banking activities, including the establishment of specific accountability, policies and controls to manage these risks.

2. *Establishment of a comprehensive security control process.*
   The board of directors and senior management should review and approve the key aspects of the BFI's security control process.

3. *Comprehensive due diligence and management oversight process for outsourcing relationships and other third-party dependencies.*
The board of directors and senior management should establish a comprehensive and ongoing due diligence and oversight process for managing the BFI's outsourcing relationships and other third-party dependencies supporting e-banking.

5.3 Security Controls (Principles 4 to 10):

4. *Authentication of e-banking customers.*
BFIs should take appropriate measures to authenticate the identity and authorisation of customers with whom it conducts business over the Internet.

5. *Non-repudiation and accountability for e-banking transactions.*
BFIs should use transaction authentication methods that promote non-repudiation and establish accountability for e-banking transactions

6. *Appropriate measures to ensure segregation of duties.*
BFIs should ensure that appropriate measures are in place to promote the adequate segregation of duties within e-banking systems, databases and applications.

7. *Proper authorisation controls within e-banking systems, databases and applications.*
BFIs should ensure that proper authorisation controls and access privileges are in place for e-banking systems, databases and applications.

8. *Data integrity of e-banking transactions, records, and information.*
BFIs should ensure that appropriate measures are in place to protect the data integrity of e-banking transactions, records and information.

9. *Establishment of clear audit trails for e-banking transactions.*
BFIs should ensure that clear audit trails exist for all e-banking transactions.

10. *Confidentiality of key bank information.*
BFIs should take appropriate measures to preserve the confidentiality of key e-banking information. Measures taken to preserve confidentiality should be commensurate with the sensitivity of the information being transmitted and/or stored in databases.

5.4 Legal and Reputational Risk Management (Principles 11 to 14):

11. Appropriate disclosures for e-banking services.
BFIs should ensure that adequate information is provided on their websites to allow potential customers to make an informed conclusion about the bank's identity and regulatory status of the bank prior to entering into e-banking transactions.

12. Privacy of customer information.
BFIs should take appropriate measures to ensure adherence to customer privacy requirements applicable to the jurisdictions to which the bank is providing e-banking products and services.

13. Capacity, business continuity and contingency planning to ensure availability of e-banking systems and services.
BFIs should have effective capacity, business continuity and contingency planning processes to help ensure the availability of e-banking systems and services.

14. Incident response planning.
BFIs should develop appropriate incident response plans to manage, contain and minimise problems arising from unexpected events, including internal and external attacks that may hamper the provision of e-banking systems and services.

5.5 Supervisory Concerns over the IT Supervisory Framework

Supervisors are highly concerned about the operational and systemic risks, within which IT and security risks are prominent. The importance of IT in the BFIs make it necessary for supervisors to assess how well IT resources are managed and the effectiveness of controls of IT risks. Some BFIs in Nepal have their own IT or operational risk department with specialists in this field. These teams can carry out focused IT inspections on their own. They can also rely on external auditors for the assessment of IT risks.

However, the NRB supervisors, while doing supervision of BFIs, would ensure that the BFIs are in full compliance with the prevailing regulations and that the board and senior management of the BFIs have proper oversight over the banking activities. The NRB supervisors would also ensure that the IT operational policies are sufficient and the risk management system is functionally adequate to identify, measure, monitor and control IT risks. The NRB supervisors would also assess the BFI's internal control system for IT implementation and the function and role of the BFI's top level IT management committee. The supervisors also

review the IT standard operating procedure and business continuity plan of BFI and provide suggestion if anything is lacking. The supervisors would also make sure that the disaster recovery plan of the BFI is perfect and tested regularly, business secrecy is highly maintained, the terms and conditions of the outsourcing is adequate and BFI-friendly and the cost of maintenance is suitable for the business size and revenue.

5.6 Status of Regulatory Framework and Regulations in Nepal

The following table shows the status of the IT supervisory framework in Nepal.

Figure 8
Status of IT Supervisory Framework

No.	Item	Yes/No
1	Is IT Implementation reported regularly?	No
2	Is IT audit conducted?	No
	- By bank/IT supervisors from supervisory authority	No
	Off-site	No
	On-site	No
	- By internal or external (third party) auditors (on-site)	No
	- Special IT audit/examination outside regular examination (on-site)	No
3	Does the formal framework exist?	No
4	If yes, is it stipulated in a regulation?	
5	Is there minimum requirement in IT Implementation?	No
	Are the following items implemented: Active supervision by Top Management (IT Steering Committee)	No
	IT Policy and Standard Operating Procedure	No
	IT risk is included in the risk-based management	No
	System development life cycle	No
	All layers of IT system	No
	Internal control system for IT Implementation	No
	Business Continuity Plan and Disaster Recovery Plan	No

	Periodical IT audit (internal/external)	No
6	Because it involves supervision procedure, is IT outsourcing especially regulated?	No
7	Because it involves consumer protection, is e-banking products especially regulated?	No
8	Are any IT-related laws (cyber law, e-commerce, m-commerce, digital signature) installed?	No

5.7 Orientation for the Prevailing Supervisory Framework

It is mentioned earlier that there is no formal supervisory framework for IT supervision. The NRB, while working towards the formulation of an IT supervisory framework, would follow the basic frame of reference provided by the BIS principles on risk management for electronic banking and the regulation and supervisory framework as applied in SEACEN member countries. The best practices in IT implementation around the world would also be reviewed while formulating the regulation and supervisory framework in Nepal. The outcome and suggestions of this research project would also be relevant for the NRB in its formulation of new regulation and development supervisory framework for IT-related banking transactions in Nepal.

5.8 IT Supervisory and Audit Practices

To date, IT audit is not practiced in the Nepalese banking system and there is no clear vision and plan for implementing the same. The non-practice of IT audit increases the overall risk profile of IT implementation in the Nepalese BFIs. It also threatens compliance with the legal and regulatory requirements as well as the confidentiality, integrity, reliability and availability of information resources. The IT supervision in BFIs is conducted along with the normal overall supervision by including an IT professional in the supervision team, and supervision is focused on the 14 principles issued by BIS.

5.9 IT-specialised Supervisors/Auditors

The Nepalese financial sector lacks certified system auditors for IS audit. Only few commercial banks conduct IS audit by professional IS auditors. The NRB also does not have certified IS auditors for conducting its supervision activities and it has not yet initiated any move towards developing such professionals. The NRB has appointed few IT graduates (Bachelors in IT Management and Bachelors in hardware or software engineering) in recent years and placed one IT officer each in two of its supervision departments. To date, the IT supervisory training program has not been conducted in the NRB.

5.10 Coordination among BFIs Authorities

Coordination among the BFIs authorities is significantly lacking. Comprehensive regulatory frameworks need to be developed to cope with all the prevailing risks arising from the use of IT as a channel for service delivery.

Figure 9
Status of IT Audit

No.	Item	Yes/No
1	Is it conducted regularly?	No
2	If not regularly, is it conducted case by case?	No
3	If regularly, objects of audit:	
	Organisation and Management	
	System development process	
	Operation	
	Software and Application, including e-Banking	
	Security (authentication, authorisation and protection – including audit trails, encryption)	
	BCP/DRP	
	Communication Network	
	Outsourcing process	
	Internal Auditing	

6. Issues And Challenges

6.1 Issues

The primary issues regarding IT supervision in Nepal are listed as follows:

6.1.1 Lack of IT Supervisory Framework

Due to the lack of supervisory framework, there is no standardised IT supervision process, which is making the supervision process extremely difficult.

6.1.2 Lack of IT Implementation Standards for BFIs

Due to the lack of IT implementation standards, it is difficult for the findings obtained from the supervision to be enforced and the heterogenous IT implementation practices is making the supervision process more complex.

6.1.3 Lack of Legal Environment to Support IT Risk Management

The following issues have been identified regarding infrastructure and technology:

- Undeveloped legal policy for electronic payment and security issues.
- Multiple issues of trust and lack of payment gateways (privacy of personal and business data connected over the Internet not assured; security and confidentiality of data not in place).
- Lack of by-laws on ETA (electronic transaction act), on security.

6.1.4 Low Level of Awareness of IT Risk and Non-acceptance of IT Audit as Necessary Supervisory Process

Most of the BFI's board of directors and senior management lack effective management oversight over the risks associated with e-banking activities, including the establishment of specific accountability, policies and controls to manage these risks. The board and senior management pay little attention towards IT activities and the risks associated with technology and the necessity of IT audit has not been felt.

6.1.5 Implementation of IT Systems Without Proper Planning and Cost-benefit Analysis

Many BFIs are using IT systems without adequate planning and cost-benefit analysis. Most of the BFIs suffer from the demonstration effect while applying IT systems in their operations. Most of the BFIs also lack skilled human resources to manage their IT systems internally. They exhibit a high degree of dependence on external vendors for their internal IT operations which increases significantly the exposure of the BFIs to the inherent risks.

6.1.6 Inadequate Staff for IT Supervision

The NRB does not have sufficient skilled human resources for IT supervision. The Bank Supervision Department and the Financial Institution Supervision Department are conducting e-banking supervision activities with a single supervisor emplaced in each of the department.

6.1.7 Lack of Standard Qualification and Training for IT Supervisors

BFIs lack certified professionals like CISA, CISSP, etc., and they have not initiated any move towards providing these types of professional training for capacity-building.

6.1.8 Lack of Sufficient IT infrastructure

The following issues have been identified regarding infrastructure and technology:

- Poor telecommunication infrastructure (slow Internet connectivity, costly and unreliable connections)
- Limited e-security knowledgeable resources in the country.
- Lack of certification authority and public key infrastructure (PKI).

6.1.9 Outsourcing of IT Activities

Many BFIs are highly reliant on external agencies for their key IT operations, but effective control mechanism for those operations is lacking due to absence of appropriate policy and guidelines.

6.1.10 Trust and Security

The following issues have been identified regarding trust and security:

- Low confidence in e-payment using the Internet as an alternative method of payment.
- Limited Internet access among customers (current level of Internet usage is low among businesses and users).
- Inexperience in integrating ICTs into the business process.

6.1.11 Socio-economic and Cultural Issues

The low income of the population and the prevailing shopping culture, i.e., most people prefer paying goods by cash rather than shop online.

6.2 Challenges

The following challenges have been identified in IT supervision in Nepal for strengthing the IT supervision process in the future:

- How to establish an IT supervisory framework in a heterogeneous environment of IT implementation?
- How to increase awareness about IT risks and its impact among customers, BODs, senior management and other stakeholders?
- Development of IT infrastructure in rural areas and establishment of certification authority and PKI.
- Understanding IT process.
- Understanding IT-supported product mechanism.
- Assessing IT risks.

- Increasing the competence of bank supervisors in IT auditing.
- Improving trust and security among customers.
- Preventing frauds.
- Potential systemic risk from IT implementation.

7. Policy Recommendations

7.1 Policy Suggestions

In Nepal, the use of IT by the BFIs is rapidly increasing. It behooves the NRB to provide for the proper regulation and supervision of the IT-related banking and financial activities. The board and senior management of the BFIs should also monitor the IT-based operations and assess the risks thereof. If the BFI management is able to control the risk in the BFIs operation, it would enhance people's confidence in the BFIs and increase the credibility of the Nepalese banking and financial system. As the NRB supervisors are conducting IT supervision in the absence of formal IT regulation and IT supervisory framework in Nepal, measures should promptly be taken to control the impact of IT implementation in the BFIs and reduce the IT-related risks in the Nepalese banking system.

- IT supervisory framework in Nepal needs to be developed without delay for the standardisation of the supervision process and to ensure risk-based management in the overall IT-related activities.

- IT standards in Nepal and the SEACEN region need to be developed for proper IT implementation in the BFIs.

- Effective formulation and implementation of cyber-law, electronic transaction act, and other necessary legislation as required for efficient banking transactions and service delivery.

- Government should develop a policy for developing IT infrastructure in the country.

- Awareness programmes to be initiated to create awareness of IT risks among the top management of the BFIs.

- Policy needs to be developed for strengthing the competency and capacity of BFI supervisor and IT auditor.

- Frequent seminars, training programmes and other necessary activities to be conducted, through the joint effort of all SEACEN members, to bring IT to a level playing field.

7.2 Specific Focus and Concluding Remarks

The use of IT in the BFIs has been changing the supervisory and regulatory landscape. It is creating new tools for supervisors and posing new supervisory challenges. Technology-driven issues, such as privacy and the nature of electronic communications, have reached the forefront of the policy agenda, with the demarcation line between electronic banking and electronic commerce becoming increasingly difficult to define clearly.

Apart from these, the Nepalese BFIs are facing innumerable challenges, such as the worrisome level of non-performing assets, deteriorating asset quality, increasing pressures on profitability, asset-liability management, liquidity-risk management, and market-risk management. Moreover, the disclosure requirements are also increasing.

The solution in overcoming the challenges would be to invest in IT. In the meantime, better use of the available information from the existing management information systems (MIS) of the the BFIs will facilitate the flow of information, and hence ease the regulation and supervision of BFIs.

The ICT revolution has lowered very significantly the transaction and coordination costs and made possible the "economically efficient" deposit-taking and lending activities. However, with the decline in transaction costs and the commoditisation of credit information, the synergies that may have existed for the BFIs to make loans to its depositors have been largely eroded.

In conclusion, the BFIs will continue experimenting with new technologies and electronic, information-based services. This is an area with great potential, yet the uncertainties are large and the payoff horizon is unknown. The BFIs and supervisors need to recognise that it is acceptable and even expected to make some investments that do not pay off. The computers and websites foul up occasionally and e-mail gets lost. The new Internet world is an unforgiving one for these routine mistakes and the BFIs have strong incentives to take precautions and to fix problems well before they reach supervisors' and policymakers' attention. The information-based nature of financial services is unlikely to change. The BFIs will continue to find new and better ways to put technology to their and their customers' best use and that they will manage the technology and the business risks associated with these investments.

Keeping in view all the above, it is necessary for Nepal to have an adequate IT regulatory and supervisory framework for establishing risk-based management in the BFIs. To strengthen the supervisory capacity of the NRB and enhance public confidence in the Nepalese banking system, the implementation of IT in the BFIs should be regulated and supervised, guided by a structured regulatory and supervisory framework, in order that the country can have a resilient banking system.

References

Banking and Financial Statistics, Nepal Rastra Bank, July 2008.

Current Macroeconomic Situation, Nepal Rastra Bank, August 2008.

IT Examination Handbook, Federal Financial Institutions Examination Council (FFIEC), USA.

"Management and Supervision of Cross-Border Electronic Banking Activities", Electronic Banking Group of the Basel Committee on Banking Supervision, BIS, July 2003.

"Risk Management Principles for Electronic Banking", Electronic Banking Group of the Basel Committee on Banking Supervision, BIS, July 2003.

Abbreviations

ABB	Any Branch Banking
ADSL	Asymmetric Digital Subscriber Line
ATM	Automatic Teller Machine
BAFIA	Banks and Financial Institutions Act, 2006
BFIs	Banks and Financial Institutions
BSD	Bank Supervision Department
DSAT	District Satellite Trunk
EFT	Electronic Fund Transfer
FISD	Financial Institutions Supervision Department
Gbps	Giga-bytes per second
ICT	Information and Communication Technology
IS	Information Security
IT	Information Technology
LAN	Local Area Network
NEPSE	Nepal Stock Exchange
NGOs	Non-Government Organizations
NRB	Nepal Rastra Bank
PKI	Public Key Infrastructure
PoS	Point of Sales
RSAT	Regional Satellite Trunk
RTGS	Real Time Gross Settlement System
SDH	Synchronous Digital Hierarchy
SEACEN	South East Asian Central Banks
SEBON	Securities Board of Nepal
SMS	Short Message Service
VSAT	Very Small Aperture Terminal
WLL	Wireless Local Loop

Appendix 1

List of Banks and Financial Institution in Nepal Commercial Banks

S.N.	Names	Operation Date (A.D.)	Head Office	Paid up Capital *(Rs. In Million)*
1	Nepal Bank Limited	1937/11/15	Kathmandu	380.4
2	Rastriya Banijya Bank	1966/01/23	Kathmandu	1172.3
3	Agriculture Development Bank Limited	1968/01/02	Kathmandu	9278.0
4	NABIL Bank Limited	1984/07/16	Kathmandu	689.2
5	Nepal Investment Bank Limited	1986/02/27	Kathmandu	1002.6
6	Standard Chartered Bank Nepal Limited.	1987/01/30	Kathmandu	620.8
7	Himalayan Bank Limited	1993/01/18	Kathmandu	1013.5
8	Nepal SBI Bank Limited	1993/07/07	Kathmandu	874.5
9	Nepal Bangladesh Bank Limited	1993/06/05	Kathmandu	744.1
10	Everest Bank Limited	1994/10/18	Kathmandu	831.4
11	Bank of Kathmandu Limited	1995/03/12	Kathmandu	603.1
12	Nepal Credit and Commerce Bank Limited	1996/10/14	Siddharthanagar, Rupendehi	1399.6
13	Lumbini Bank Limited	1998/07/17	Narayangadh, Chitawan	996.3
14	Nepal Industrial & Commercial Bank Limited	1998/07/21	Biaratnagar, Morang	943.8
15	Machhapuchhre Bank Limited	2000/10/03	Pokhara, Kaski	821.7
16	Kumari Bank Limited	2001/04/03	Kathmandu	1478.5
17	Laxmi Bank Limited	2002/04/03	Birgunj, Parsa	915.0
18	Siddhartha Bank Limited	2002/12/24	Kathmandu	828.0
19	Global Bank Ltd.	2007/01/02	Birgunj, Parsa	1000.0
20	Citizens Bank International Ltd.	2007/6/21	Kathmandu	700.0
21	Prime Bank Ltd	2007/9/24	Kathmandu	700.0
22	Sunrise Bank Ltd.	2007/10/12	Kathmandu	700.0
23	Bank of Asia Nepal Ltd.	2007/10/12	Kathmandu	700.0
24	Development Credit Bank Ltd	2008/05/25	Kathmandu	1100.0
25	NMB Bank Ltd.	2008/06/02	Kathmandu	1000.0

Development Banks

S.No	Names	Operation Date (A.D.)	Head Office	Paid up Capital (Rs. In Million)
1	Nepal Industrial Development Corporation	1959/06/15	Durbar Marg, Kathmandu	415.8
2	Nepal Development Bank Ltd.	1999/01/31	Kamaladi, Kathmandu	320.0
3	Uddyam Development Bank Ltd.	1999/02/22	Tandi, Chitawan	17.5
4	Malika Development Bank Ltd.	1998/12/27	Dhangadhi, Kailali	50.0
5	Siddhartha Development Bank Ltd.	1998/08/20	Butawal-11, Rupandehi	107.6
6	United Development Bank Ltd.	2002/03/16	Jeetpur, Bara	14.0
7	Nepal cottage and Small Ind. Dev. Bank Ltd.	2001/06/19	Heritage Plaza, Kathmandu	112.0
8	Narayani Development Bank Ltd.	2001/10/17	Ratna Nagar-1, Chitawan	25.0
9	Pashimanchal Development Bank Ltd.	2003/3/2	Butawal-8, Rupandehi	100.0
10	Sahayogi Bikas Bank Ltd.	2003/10/21	Janakpurdham,Dhanusha	20.0
11	Pashupati Development Bank Ltd.	2004/01/01	Banepa, Kavre	120.0
12	Karnali Bikash Bank Ltd.	2004/02/14	Nepalgunj, Banke	25.1
13	Triveni Development Bank Limited	2004/07/26	Bharatpur, Chitawan	35.0
14	Annapurna Development Bank Limited	2004/08/23	Banepa, Kavre	192.0
15	Bhrikuti Bikas Bank Limited	2004/08/19	Butawal, Rupandehi	58.8
16	Shubhechchha Bikas Bank Limited	2004/09/14	Narayangadh, Chitawan	23.9
17	Bageshowri Bikas Bank Limited	2004/10/19	Nepalgunj, Banke	30.0
18	Sanima Bikas Bank Limited	2004/11/26	Nagpokhari, Kathmandu	384.0
19	Gaurishankar Bikas Bittiya Sanstha Ltd.	2004/11/29	Kawasoti, Nawalparasi	18.3
20	Gorkha Bikas Bank Limited	2004/12/01	Putalisadak, Kathmandu	480.0
21	Gandaki Development Bank Ltd.	2005/01/19	Pokhara, Kaski	82.3
22	Infrastructure Development Bank Ltd.	2005/04/29	Banepa, Kavre	80.0
23	Business Development Bank Ltd.	2005/05/10	Pokhara, Kaski	210.0
24	Biratlaxmi Bikas Bank Limited	2005/05/11	Biratnagar, Morang	50.0
25	Excel Development Bank Ltd.	2005/07/21	Anarmani,Jhapa	20.0
26	Western Development Bank Ltd.	2005/09/15	Tribhuvannagar, Dang	16.2
27	Himchuli Bikas Bank Limited	2005/11/07	Pokhara, Kaski	90.0
28	Arniko Bikas Bank Ltd.	2006/07/06	Dhulekhel, Kavre	27.1
29	Nepal Dev. and Employment Promotion Bank Ltd.	2006/07/17	Kamaladi, Kathmandu	320.0
30	Clean Energy Development Bank Ltd.	2006/09/06	Sitapaila, Kathmandu	320.0
31	Mitery Development Bank Ltd.	2006/10/13	Mahendrapath-5, Dharan	31.6
32	Tinau Bikas Bank Ltd.	2006/10/13	Sangampath, Butwol	21.0
33	Gaindakot Development Bank Ltd.	2006/12/18	Navalparasi, Gaindakot	24.2
34	Muktinath Bikas Bank Ltd.	2006/12/18	Putalibazar, Syanja	52.0
35	Sewa Bikas Bank Ltd.	2007/2/25	Butawal, Rupandehi	41.1
36	Kankai Bikas Bank Ltd.	2007/5/4	Damak, Jhapa	28.0
37	Public Development Bank Ltd.	2007/6/7	Birjunj, Parsa	45.0
38	Mahakali Bikas Bank Ltd.	2007/8/18	Mahendranagar, Kanchanpur	11.8
39	Ace Development Bank Ltd.	1995/08/15	Narayanchaur, Kathmandu	416.0

40	Sangrila Bikas Bank Ltd.	2007/8/26	Pokhara, Kaski	39.9
41	Bhargab Bikas Bank Ltd.	2007/8/30	Nepalgunj, Banke	12.0
42	Vibor Bikas Bank Ltd.	2007/10/4	Tripureshwor, Kathmadu	414.8
43	Resunga Bikas Bank Ltd.	2007/9/26	Tamghas, Gulmi	13.4
44	Rara Bikas Bank Ltd.	2007/9/30	Birendranagar, Surkhet	10.0
45	Diyalo Bikas Bank Ltd.	2007/10/01	Banepa, Kavre	38.9
46	Country Development Bank Ltd.	2007/10/04	Banepa, Kavre	51.0
47	Kasthamandap Development Bank Ltd.	2007/10/25	New Road, Kathmandu	224.0
48	Alpine Development Bank Ltd.	2007/10/05	Hetauda, Makawanpur	33.2
49	Nilgiri Bikas Bank Ltd.	2007/10/25	Beni, Maygdi	10.5
50	Corporate Development Bank Ltd.	2007/10/25	Birjung, Parsa	68.4
51	Kamana Bikas Bank Ltd.	2007/9/29	Lekhnath, Kaski	26.0
52	City Development Bank Ltd.	2007/10/19	Pokhara, Kaski	35.0
53	Garima Bikas Bank Ltd.	2007/11/23	Sangja	26.5
54	Biswo Bikas Bank Ltd.	2007/11/21	Pokhara, Kaski	73.2
55	Pathibhara Bikas Bank	2007/11/21	Urlabari, Morang	25.5
56	Professional Bikas Bank Ltd.	2007/10/17	Banepa, Kavre	35.0
57	Kabeli Bikas Bank Ltd.	2007/11/15	Dhankuta	10.1
58	Purnima Bikas Bank Ltd.	2008/5/20	Sidhardhanagar, Rupandehi	26.9
59	Jyoti Development Bank Ltd.	2008/8/25	Kamalpokhari, Kathmandu	259.0

Finance Companies

S. No.	Names	Operation Date (A.D.)	Head Office	Paid up Capital (Rs. In Million)
1	Nepal Housing Development Finance Co.Ltd.	1992/03/08	Naya Baneshwor, Kathmandu	70.5
2	Nepal Finance Co. Ltd.	1993/01/06	Kamaladi, Kathmandu	45.0
3	NIDC Capital Markets Ltd.	1993/03/11	Kamaladi, Kathmandu	101.2
4	National Finance Co.Ltd.	1993/05/07	Pako Newroad, Kathmandu	156.9
5	Annapurna Finance Co.Ltd.	1993/09/30	Chipledhunga, Pokhara	201.6
6	Nepal Share Markets and Finance Ltd.	1993/10/19	Ramshahapath, Kathmandu	432.0
7	Peoples Finance Ltd.	1993/04/15	Tripureshwor, Kathmadu	84.0
8	Mercentile Finance Co. Ltd.	1994/11/10	Birgunj, Parsa	18.0
9	Kathmandu Finance Ltd.	1994/11/10	Putalisadak, Kathmandu	38.0
10	Himalaya Finance & Savings Co.Ltd.	1993/11/11	Sundhara, Kathmandu	48.0
11	Union Finance Ltd.	12/12/1995	Ganeshwor, Kathmandu	72.5
12	Narayani Finance Ltd.	1995/03/08	Narayangadh, Chitwan	213.7
13	Gorkha Finance Ltd.	1995/03/12	Hattisar, Kathmandu	59.6
14	Paschhimanchal Finance Co.Ltd.	1995/04/09	Butawal, Rupendehi	100.0
15	Nepal Housing & Merchant Finance Co.Ltd.	1995/04/11	Dillibazar, Kathmandu	80.4
16	Universal Finance Co.Ltd.	1995/04/27	Kantipath, Kathmandu	60.2
17	Samjhana Finance Co. Ltd.	1995/05/03	Banepa, Kavre	23.4
18	Goodwill Finance Ltd.	1995/05/16	Dillibazar, Kathmandu	105.0
19	Siddhartha Finance Co. Ltd.	1995/05/25	Siddarthanagar, Rupendehi	67.7

20	Shree Investment & Finance Co. Ltd.	1995/06/01	Dillibazar, Kathmandu	84.0
21	Lumbini Finance & Leasing Co. Ltd.	1995/06/26	Thamel, Kathmandu	90.0
22	Inbesta Finance Ltd.	1995/07/17	Birgunj, Parsa	24.0
23	Yeti Finance Co. Ltd.	1995/07/23	Hetauda, Makawanpur	31.3
24	Standard Finance Ltd.	1995/07/23	Pautalisadak, Ktm.	144.8
25	International Leasing & Finance Co. Ltd.	1995/10/31	Naya Baneshwor, Ktm.	144.0
26	Mahalaxmi Finance Co. Ltd.	1995/11/26	Birgunj, Parsa	80.0
27	Lalitpur Finance Co. Ltd.	1995/12/12	Lalitpur	75.9
28	Bhajuratna Finance & Saving Co. Ltd.	1996/01/09	Kantipath, Kathmandu	38.5
29	United Finance Ltd.	1996/1/25	Kamaladi, Kathmandu	145.0
30	General Finance Ltd.	1996/02/02	Chabahil, Kathmandu	24.2
31	Nepal Shreelanka Merchant Bank Ltd.	1996/02/04	Kamaladi, Kathmandu	100.0
32	Merchant Finance Co. Ltd.	1996/01/02	Kathmandu	30.0
33	Alpic Everest Finance Ltd.	1996/07/16	Baghbazar, Kathmandu	78.0
34	Nava Durga Finance Co.Ltd.	1997/02/09	Itachhe, Bhaktapur	45.6
35	Janaki Finance Ltd.	1997/03/07	Janakpurdham, Dhanusha	40.0
36	Pokhara Finance Ltd.	1997/03/16	Pokhara, Kaski	60.0
37	Central Finance Co. Ltd.	1997/04/14	Kupondole, Lalitpur	72.0
38	Premier Finance Co. Ltd.	1997/05/08	Manbhavan, Lalitpur	28.8
39	Arun Finance & Saving Co. Ltd.	1997/08/17	Dharan, Sunsari	11.0
40	Multipurpose Finance Co. Ltd	1998/3/25	RajbiRaj, Saptari	3.0
41	Butwal Finance Co. Ltd.	1998/06/21	Butawal, Rupendehi	69.7
42	Shrijana Finance Ltd.	1999/12/14	RajbiRaj, Saptari	14.0
43	Om Finance Ltd.	2000/09/17	Pokhara, Kaski	70.0
44	Cosmic Merchant Banking & Finance Ltd.	2000/11/20	Lal Durbar Marg, Ktm.	75.1
45	World Merchant Banking & Finance Ltd.	2001/08/10	Hetauda, Makawanpur	72.0
46	Capital Merchant Banking & Finance Ltd.	2002/02/01	Battisputali, Kathmandu	346.2
47	Crystal Finance Ltd.	2002/02/13	Bag Durbar, Kathmandu	49.0
48	Royal Merchant Banking & Finance Ltd.	2002/02/14	Durbarmarg, Kathmandu	122.0
49	Guheshworil Merchant Banking & Finance Ltd	2002/06/13	Jawalakel, Lalitpur	61.7
50	Patan Finance Ltd.	6/23/2002	Man Bhawan, Lalitpur	50.0
51	Kist Merchant Banking & Finance Ltd.	2003/02/21	Kamalpokhari, Kathmandu	800.0
52	Fewa Finance Ltd.	2003/04/30	Pokhara, Kaski	70.0
53	Everest Finance Co. Ltd.	2003/07/02	Bhairahawa, Rupendehi	20.0
54	Birgunj Finance Ltd.	9/28/2003	Birgunj, Parsa	72.6
55	Prudential Bittiya Sanstha Ltd	2003/06/06	Dillibazar, Kathmandu	100.0
56	ICFC Bittiya Shanstha Ltd.	2003/06/15	Bhatbhateni, Kathmandu	299.4
57	IME Financial Institution Ltd.	2005/08/01	Kantipath, Kathmandu	82.5
58	Sagarmatha Merchant Banking and Finance Co	2005/08/29	Maanvawan, Lalitpur	50.0
59	Shikhar Bittya Sanstha Ltd.	2005/09/15	Thapathali,Kathmandu	30.0
60	Civil Merchant Bittiya sanstha Ltd.	2005/09/18	Kuleshwor,Kathmandu	50.0
61	Prabhu Finance Co. Ltd.	2006/02/16	Kantipath,Kathmandu	85.0
62	Imperial Financial Institution Ltd.	2006/03/08	Putalisadak,Kathmandu	50.0
63	Kuber Merchant Bittiya sanstha Ltd.	2006/03/24	Putalisadak,Kathmandu	50.0
64	Nepal Express Finance Ltd.	2006/05/04	Butawal, Rupendehi	80.0
65	Valley Finance Ltd.	2006/05/11	Maharajganj, Kathmandu	27.5
66	Seta Bittiya sanstha Ltd.	2006/06/07	Tikapur, Kailali	5.2
67	Hama Financial Institution Ltd.	2006/06/16	Tripureshwor, Kathmandu	31.5

68	Reliable Investment Bittiya sanstha Ltd.	2006/09/06	Sundhara, Kathmandu	95.4
69	Loard Buddha Financial Institutions Ltd.	2006/11/19	Newroad, Kathmandu	51.6
70	Api financial Institution Ltd.	2007/4/25	Lekhanath Chock, Kaski	42.0
71	Namaste Bitiya Sanstha Limited.	2007/07/07	Ghorai, Dang	10.1
72	Kaski Finance Limited	2007/7/30	Pokhara, Kaski	30.0
73	Suryadarshan Financial Institution Ltd.	2007/7/30	Baneshor, Kathmandu	30.0
74	Zenieth Merchant Financial Institution Ltd.	2007/10/08	Newroad, Kathmandu	57.0
75	Unique Financial Institution Ltd.	2007/10/12	Putalisadak, Kathmandu	30.0
76	Manjushree Financial Institution Ltd.	2007/10/15	New Baneshor, Kathmandu	70.0
77	Swostik Merchant Finance Company Ltd.	2007/10/16	Kichapokhari, Kathmandu	31.8
78	Subhalaxmi Finance Ltd.	2007/11/11	Naxal, Kathmandu	70.0

Micro-Credit Development Banks

S. No.	Names	Operation Date (A.D.)	Head Office	Paid up Capital (Rs. In Million)
1	Purbanchal Grameen Bikas Bank	1993/03/28	Biratnagar, Morang	60.0
2	Sudur Pashimanchall Grameen Bikas Bank	1993/03/28	Dhangadhi, Kailali	58.5
3	Pashimanchall Grameen Bikas Bank	1995/04/01	Butawal-8, Rupendehi	60.0
4	Madhya Pashimanchal Grameen Bikas Bank	1995/04/01	Nepalgunj, Banke	60.0
5	Madhymanchall Grameen Bikas Bank	1996/07/08	Janakpur, Dhanusha	60.0
6	Nirdhan Utthan Bank Ltd.	1999/04/13	Bhairahawa, Rupandehi	71.9
7	Rural Microfinance Development Centre	1996/12/06	Putalisadak, Kathmandu	250.0
8	Deprosc Development Bank Ltd.	2001/07/03	Ratnanagar, Chitwan	22.6
9	Chhimek Development Banks Ltd.	2001/12/10	Hetauda - 4,Makawanpur	51.0
10	Shawalamban Laghu Bitta Bikas Banks Ltd	2002/02/22	Janakpur, Dhanusha	25.0
11	Sana Kisan Vikas Bank Ltd.	2002/03/11	Bijulibazar, Kathmandu	119.8
12	Nerude Laghu Bitta Bikas Bank Ltd.	2007/06/07	Biratnagar, Morang	7.0

Savings and Credit Co-operatives (Limited Banking)

S. No.	Names	Operation Date (A.D)	Head Office	Paid up Capital *(Rs. In Million)*
1	Nabajivan Co-operative Ltd.	1993/12/15	Dhangadi, Kailali	18.6
2	Sagun Co-operative Society Ltd.	1994/10/9	Kathamandu	11.9
3	Nepal Co-operative Society Ltd.	1994/12/30	Kathamandu	31.1
4	The Sahara Loan,Savings & Investment Co-op.Soc. Ltd.	1995/04/15	Sarlahi	29.2
5	Bindabasini Saving Fund Co-operative Society Ltd.	1995/06/21	Khopasi, Kavre	18.1
6	Mahila Co-operative Society Ltd.	1995/09/27	Kathmandu	12.6
7	Bahooddeshya Saving & Loan Co-op.Society Ltd.	1995/12/25	Jhapa	19.0
8	Rajshree Saving & Invest.Co-op Society Ltd	1996/02/19	Sarlahi	29.4
9	Sahakari Bittiya Sanstha Ltd.	1696/6/16	Nepalgunj, Banke	8.3
10	Manakamanal Sahakari Sanstha Ltd.	1997/02/18	Banepa, Kavre	11.5
11	Very Co-operative Sanstha Ltd.	1997/12/25	Kathmandu	6.6
12	Viccu Saving & Loan Co-operative Sanstha	1997/02/18	Banepa, Kavre	4.6
13	Kisan Bahoo-uddesyiya Co-op. Sanstha Ltd.	1997/08/11	Lamki,Kailali	4.6
14	Himalaya Co-operative Ltd.	1998/12/29	Old Baneshowar, Ktm	45.9
15	Star Bahoo-Uddesyiya Saving & Credit Co-op Ltd.	1998/02/13	Biratnagar, Morang	5.0
16	Upakar Savings & Credit Co-operative So. Ltd.	1998/04/14	Walling, Sanja	11.6

Non-Government Organizations (NGOs)

S. No.	Names	Operation Date (A.D)	Head Office	Fund & Reserves *(Rs. in Thousand)*
1	Nepal Grameen Bikas Sanstha	2000/06/05	Kathmandu	-
2	Nepal Sikara Grameen Bikas Karyakram	2000/06/05	Chitwan	522
3	Chartare yuba Club	2000/06/05	Baglung	110
4	Mahuli Samudyik Bijkas Kendra	2000/06/12	Saptari	2881
5	United Youth Community (UNYC NEPAL)	2000/06/29	Bardiya	-
6	Samudayik Mahila Bikas Kendra	2000/07/14	Saptari	-
7	Grameen Samudayako Lagi yojana Pratavuti, Nepal	2000/08/23	Dhankuta	-
8	Grameen Jagaran Manch (Programm Co-ordination Office)	2000/09/11	Baglung	156
9	Sarbodaya Grameen Bikas Sangh	2000/09/26	Saptari	-
10	Jan Jagaran Manch	2000/10/26	Rasuwa	111
11	Rastriya Shaichik Tatha Samajik Bikas Sanstha	2000/10/01	Parbat	-
12	Dhaulagiri Community Researh Dev. Centre	2000/10/21	Baglung	-
13	Nepal Enviroment & Pollution Eradication UNESCO Nepal	2001/07/05	Gangabu	127
14	Society of Local Volunteers Efforts Nepal (Solve)	2001/07/10	Dhankuta	519
15	Women Enterprises Association of Nepal	2001/09/24	Kathmandu	1146
16	Center for Women's Right and Development	2002/04/30	Kathmandu	-
17	MANUSHI	2002/05/03	Kathmandu	1462
18	Life Development Society	2002/06/18	Morang	-
19	Women Development and Child Care Foundation	2002/07/02	Saptari	-
20	Mahila Adarsha Sewa Kendra	2002/07/02	Kthmandu	620
21	Patan Buisiness and Professional Women	2002/07/02	Lalitpur	-
22	Women Development Centre	2002/07/02	Chitwan	-
23	Womens Self -Relient Society	2002/07/14	Chitwan	-
24	Women Development Centre of Nepal	2002/07/12	Lalitpur	650
25	Bhagawan Youth Club, Alapot, Ktm.	2002/07/23	Kathmandu	35
26	Creative Women Environment Development Association.	2002/07/24	Kathmandu	730
27	Srijana Community Development Center,Siraha	2002/07/25	Siraha	-
28	Shreejana Development Center,Kaski	2002/08/22	Kaski	2090
29	Cottage & Small Industries Organization,Kathmandu	2002/09/02	Kathmandu	-
30	Rural Area Dev. & Research Programme,Parbat	2002/09/03	Parbat	-
31	Adarsha Yuba Club,Bhaktapur	2002/09/06	Bhaktapur	-
32	Society Welfare Action Nepal (SWAN),Dang	2002/10/25	Dang	-

33	Social Upgrade in Progress of Education Region (SUPER)	2002/10/29	Dang	-
34	Nepal Women Community Service Center,Dang	2002/10/30	Dang	-
35	Forum for Rural Women Ardency Development,(FORWARD)	2002/12/30	Sunsari	-
36	Gramin Mahila Bikash Sanstha	2003/04/23	Dang	-
37	Ama Samaj Shangh,Chitawan	2003/04/29	Chitwan	15
38	Gramin Mahila Utthan Kendra,Dang	2003/06/18	Dang	-
39	Khurkot Youba Club ,Parbat	2003/09/14	Parbat	-
40	Gramin Sewa Nepal	2003/09/18	Kailali	247
41	Nari Avudya Kendra	2003/10/24	Chitwan	-
42	Mahila Upakar Manch	2003/10/29	Banke	2131
43	Chhimek Samaj Sewa Sanstha	2004/09/29	Kathmandu	8886
44	Sawabalamban Bikash Kendra	2004/11/01	Kathmandu	57390
45	Bikash Aayojana Sewa Kendra	2004/11/01	Kathmandu	72500
46	Gramin Swayam Sewak Samaj	2005/11/20	Hariwon,Sarlahi	1955

CHAPTER 8

THE SUPERVISORY IMPACT OF TECHNOLOGY ON SEACEN FINANCIAL INSTITUTIONS: ISSUES AND CHALLENGES IN SRI LANKA

by G.K.K. Gamage[1]

1. Introduction

1.1 Structure of the Financial System

The financial system in Sri Lanka comprises the major financial institutions, namely, the Central Bank of Sri Lanka, Licensed Commercial Banks (LCBs), Licensed Specialised Banks (LSBs), Registered Finance Companies (RFCs), Specialised Leasing Companies (SLCs), Primary Dealers (PDs), Pension and Provident Funds, Insurance Companies, Rural Banks, Merchant Banks, Unit Trusts and Thrift and Credit Co-Operative Societies, the major financial markets, such as the foreign exchange market, money market, capital market and the informal financial market, and the financial infrastructure which is the legal framework related to the financial system and the payment and settlement system.

The banking sector in Sri Lanka, which comprises LCBs and LSBs, dominates the financial system and accounted for 57% of the total assets of the financial system as at the end of September 2006. Banks play a central role within the financial system as they have the capacity to provide liquidity to the entire economy. Banks are also responsible for providing payment services, thereby facilitating all entities to carry out their financial transactions. On the other hand, banks can create vulnerabilities of a systemic nature partly due to a mismatch in maturity of assets and liabilities. Therefore, the soundness of banks is important, as it contributes towards the maintenance of confidence in the financial system and any failure may have the potential of impacting the activities of all the other financial and non-financial entities.

In terms of the asset base and the magnitude of services provided, the LCBs are the single most important category of financial institution within the banking sector. As at the end of September 2006, the LCBs dominated the financial system with a market share of 48 % of the entire financial system's assets and 84% of the banking sector's assets. Therefore, the health of the financial system depends to a large extent on the soundness of the financial institutions, particularly the LCBs.

---

1 Author is Senior Assistant Director of the Bank Supervision Department of Central Bank of Sri Lanka.

As at the end of September 2006, the banking sector comprised 23 LCBs and 14 LSBs. Even though a large number of licensed banks exist in the country, the stability of the financial system is primarily dependent on the performance and financial strength of the six largest LCBs, consisting of the two state banks and the four largest domestic private commercial banks. These six banks, which are generally referred to as the Systemically Important Banks (SIBs), represented 78 % of the LCB sector assets and 65% of the banking sector assets. In terms of deposits, the SIBs held a market share of 83% and 68% of LCB sector and banking sector deposits, respectively.

The LSB sector represented 9% and 16% of the entire financial system's assets and banking sector's assets, respectively. The systemic importance of the LSB sector is relatively low in comparison to the LCBs, both in terms of size and their impact on the financial system, as it does not play an intermediary role in the payment cycle.

2. Overview of the Financial System

2.1 Components of the Financial System

The financial system consists of the Central Bank, as the apex financial institution, other regulatory authorities, financial institutions, markets, instruments, a payment and settlement system, a legal framework and regulations. The financial system carries out the vital financial intermediation function of borrowing from surplus units and lending to deficit units. The legal framework and regulators are needed to monitor and regulate the financial system. The payment and settlement system is the mechanism through which transactions in the financial system are cleared and settled.

2.2 Regulatory Authorities

The regulation and supervision of banking institutions is mainly governed by the Monetary Law Act No. 58 of 1949, the Banking Act No. 30 of 1988, and the Exchanged Control Act No. 24 of 1953. The regulation and supervision of finance companies is carried out under the Finance Companies Act No. 78 of 1988. The regulation and monitoring of finance leasing companies is conducted under the Finance Leasing Act No. 56 of 2000. The regulation and supervision of primary dealers in government securities is carried out under the Local Treasury Bills Ordinance No. 8 of 1923 and the Registered Stocks and Securities Ordinance No. 7 of 1937.

The institutions being supervised are the systemically important institutions for financial stability. However, competition in the financial sector sometimes could make some financial institutions unviable, if they do not adapt themselves to the rapidly changing financial environment. Such institutions are either restructured or liquidated, based on the extent to which they have deteriorated.

2.3 Securities and Exchange Commission

Pursuant to the Securities and Exchange Commission of Sri Lanka Act No. 36 of 1987, the Securities and Exchange Commission (SEC) is responsible for licensing and regulating stock exchanges, stockbrokers, stock dealers and unit trust companies. The SEC also registers underwriters, margin providers, credit rating agencies, investment managers and securities clearing houses. In order to co-ordinate financial stability issues, the Central Bank is a member of the Board of Directors of the SEC and the Deputy Governor in charge of Financial System Stability represents the Central Bank on the SEC Board.

2.4 Insurance Board of Sri Lanka

The Insurance Board of Sri Lanka (IBSL) regulates and supervises the insurance industry - insurance companies and their agents and insurance brokers, under the Regulation of Insurance Industry Act No.43 of 2000 to safeguard the interests of policyholders. The Central Bank is a member of the IBSL and is represented on it by the Deputy Governor in charge of Financial System Stability.

2.5 Financial Institutions

The following are the institutions regulated by the Central Bank of Sri Lanka:

- Licensed Commercial Banks
- Licensed Specialised Banks
- Registered Finance Companies
- Registered Leasing Companies
- Authorised Primary Dealers

A law to regulate Micro-Finance Institutions is currently under preparation and it has been proposed that the Central Bank shall supervise Micro-Finance Institutions.

2.6 Institutions Not Regulated by the Central Bank of Sri Lanka

Certain financial institutions are not regulated by the Central Bank. These include the Stock Broking/Dealing Companies, Unit Trust Companies and Investment Management Companies, which come under the purview of the SEC,

Insurance Companies and Insurance Brokers, which are regulated by the IBSL, and Venture Capital Companies, Pension and Provident Funds and Micro-Finance Institutions.

2.7 Financial Markets

The Financial Market, which is the market for credit and capital, can be divided into the Money Market and the Capital Market. The Money Market is the market for short-term interest-bearing assets with maturities of less than one year, such as Treasury bills, commercial paper, and certificates of deposits. The major task of the Money Market is to facilitate the liquidity management in the economy. The main issuers in the Money Market are the Government, banks and private companies, while the main investors are banks, insurance companies and pension and provident funds. The Capital Market is the market for trading in assets for maturities of greater than one year, such as Treasury bonds, private debt securities (bonds and debentures) and equities (shares). The main purpose of the Capital Market is to facilitate the raising of long-term funds. The main issuers in the Capital Market are the Government, banks and private companies, while the main investors are pension and provident funds and insurance companies.

The Financial Market can be also be classified according to instruments, such as the debt market and the equity market. The debt market is also known as the Fixed Income Securities Market and its segments are the Government Securities Market (Treasury bills and bonds) and the Private Debt Securities Market (commercial paper, private bonds and debentures). Another distinction can also be drawn between primary and secondary markets. The Primary Market is the market for new issues of shares and debt securities, while the Secondary Market is the market in which existing securities are traded.

The Central Bank through its conduct of monetary policy influences the different segments of the Financial Market in varying degrees. The Central Bank's policy interest rates have the greatest impact on a segment of the Money Market called the inter-bank call money market and a segment of the Fixed Income Securities Market, i.e. the Government Securities Market. The Central Bank may also intervene in the inter-bank Foreign Exchange Market, which is closely connected to the Money Market.

Figure 1
Total Assets and Deposit Liabilities of the Main Financial Institutions

Total Assets and Deposit Liabilities of the Main Institutions in the Financial System as at end June 2007 1 US$ = 107 Rs				
	Assets		Deposit Liabilities	
Financial Institution	**Rs. bn.**	**% Share**	**Rs. bn.**	**% Share**
Central Bank of Sri Lanka	544.5	13.5	n.a	n.a
Institutions Regulated by the Central Bank	3,111.5	77.2	1,669.3	98.2
Deposit Taking Institutions	2,459.3	61.0	1,669.3	98.2
Licensed Commercial Banks	1,964.4	49.0	1,335.4	78.5
Licensed Specialised Banks	371.6	9.2	267.0	15.7
Registered Finance Companies	123.3	3.1	66.9	3.9
Other Institutions	652.2	16.2	n.a.	n.a.
Employees' Provident Fund	516.0	12.8	n.a.	n.a.
Primary Dealers	53.0	1.3	n.a.	n.a.
Specialised Leasing companies	83.2	2.1	n.a.	n.a.
Institutions not Regulated by the Central Bank	376.2	9.3	31.1	1.8
Deposit Taking Institutions	33.4	0.8	31.1	1.8
Rural Banks	28.5	0.7	26.4	1.6
Thrift and Credit Co-operative Societies	4.9	0.1	4.7	0.3
Contractual Savings Institutions	309.4	7.7	n.a	n.a
Employees Trust Fund	71.9	1.8	n.a	n.a
Private Provident Funds	112.6	2.8	n.a	n.a
Insurance Companies	124.9	3.1	n.a	n.a
Other Specialised Financial Institutions	33.4	0.8	n.a	n.a
Merchant Banks	31.3	0.8	n.a	n.a
Venture Capital Companies	1.4	0.0	n.a	n.a
Unit Trusts	5.2	0.1	n.a	n.a
Stock Broking Companies	4.8	0.1	n.a	n.a
Credit Rating Agencies	0.7	0.0	n.a	n.a
Total Assets	4,032.2	100.0	1,700.4	100.0

Figure 2
Capital Adequacy and NPA

Capital Adequacy and NPA	**2007 Q3**
1. Capital Adequacy Ratio - Tier I Capital Ratio (%)	11.2
2. Capital Adequacy Ratio - Total Capital Ratio (%)	12.6
3. Gross NPA as a % of Total Loans & Advances	5.4
4. Net NPA as a % of Capital Funds	13.5

Figure 3
Distribution of Banks and Bank Branches

Distribution of Banks and Bank Branches	**End 2007**
Licensed Commercial Banks (LCB) Domestic Banks Foreign Banks	23 11 12
2. Total No of LCB Branches and other outlets	4,203
3. Licensed Specialised Banks (LSB)	16
4. Total No of LSB Branches and other outlets	627
5. Total No of Automated Teller Machines (ATMs)	1,422
6. Total No of Point of Sale Machines (POS)	12,214
7. Total No of Credit Cards issued	889,780

3. Survey of the IT Implementation

Figure 4
Survey of the IT Implementation

No.	Item	Yes/No
1	Communication Network	
	Cable (Phone line)	Yes
	Satellite	Yes
	Fiber Optic	Yes
2	Use of Cellular Phone	
	Is it relatively wide spread?	Yes
3	Use of Internet	
	Is it relatively wide spread?	Yes
4	National Payment System	Yes
5	Operated by government agency / central bank	Central Bank
6	Operated by an independent or private company	
7	Automated/Computerised Payment System	Yes
8	RTGS	Yes
9	National Securities Settlement System	
	Operated by government agency / central bank	Government Agency
	Automated/Computerised Settlement System	Yes

All domestic Banks use phone lines to connect their branch systems island-wide and local branches of foreign banks use satellites and fiber optic for data communications. Most of the Commercial Banks provide Internet banking facility for their customers.

Figure 5

The Presence of Technology-supported Financial Products and Services.

No.	Item	Yes/No
1	Credit Card	
	National (only used in the country)	Yes
	International	Yes
2	Debit Card	
	National (only used in the country)	Yes
	International	Yes
3	ATM	
	Individual bank	Yes
	Nationally-Shared ATM	No
	Internationally-Shared ATM	Yes
4	Electronic Fund Transfer (EFT)	Yes
5	EFT at Point of Sale	
	National (only within the country)	Yes
	International	Yes
6	Remittance Service	
	Domestic companies	Yes
	International companies	Yes
7	Phone Banking	
	Informational	Yes
	Transactional intra bank	Yes
	Transactional inter bank	No
8	Mobile/SMS Banking	
	Informational	Yes
	Transactional intra bank	Yes
	Transactional inter bank	No
9	Internet Banking	
	Informational	Yes
	Transactional intra bank	No
	Transactional inter bank	Yes
10	Pre-paid card	Yes

Figure 6
Automated Systems

No.	Item	Yes/No
1	Core Banking: General Ledger, Third Party Fund, Loan, and Consumer Information File	Yes
2	Treasury	Yes
3	Remittance	Yes
4	Trade Finance	Yes
5	Corporate Online Service	Yes

Information system auditors and financial auditors attached to the Central Bank of Sri Lanka encounter some difficulties due to the heterogeneity of technology installed in the financial institutions.

4. Impact of IT Implementation on Financial Institutions

4.1 Management Risk

The management of a Financial Institution (FI) should properly identify, measure, monitor, and control risks associated with IT. Management should be able to distinguish risk components and to focus on risk mitigation. The board should ensure a programme exists to manage and monitor this risk. The programme should address the institution's tolerance for risk, the effectiveness of internal controls, management's accountability in regard to risk mitigation, and the processes needed to manage IT resources effectively.

It is mandatory for the FI to document a comprehensive IT policy. A Board Committee should be set up to administer all aspects of IT-related activities. The Board should ensure that the strategic plan of the bank is aligned with the IT policy of the institution and all stages of implementation, such as planning, acquiring, delivery and support, and evaluation. The responsibility of the Board of Directors and Management of a FI include:

- The selection of information architecture,
- Attention to user requirements and specifications
- Determination of the technological direction,
- IT processes and relationships,
- Management of IT investment and utilisation of IT resources, including human resources.

In order for the entire IT project to succeed, it is vital to communicate the aim and direction to the entire staff.

4.2 Operational Risk

Although management needs to be aware of all potential risks, operational risk is the primary risk associated with information technology. Operational risk is the risk of loss resulting from inadequate or failed processes, people, or systems. The root cause can be either internal or external events. Operational risk is present across all business lines. Operational risk may arise from fraud or error. Management's inability to maintain a competitive position, to manage information processing efficiently and effectively to deliver products and services can also create and compound operational risk.

Weak operational risk management can result in substantial losses from a number of IT threats including Hardware, Software or Communications failure, business disruptions or improper business practices.

Therefore, it is mandatory to provide logical and physical protection to the system. Further it is required to assure the integrity, availability and confidentiality of data.

4.3 Reputational, Compliance and Legal Risk

Inadequate attention of the Board of Directors/Management and controls over the IT systems may cause the following weaknesses, which create Reputational, Compliance and Legal risk.

- Non-availability of services
- Inefficient service
- Ineffective outcome
- Non-compliance with regulations or existing laws
- Threat to the integrity if data

In order to mitigate those risks it is required to educate and train all users. Therefore the Management of any FI should focus on training needs, execution of effective training strategy and evaluate the end results. Non-existence of established service-desk procedure to attend customer requests, incidents and service requests might deteriorate the risk status of FIs. The above risks are mainly due to non-identification of system configurations and its attributes. Proper surveys, feasibility studies and establishment of a procedure to collect suggestion from all system users are also required to mitigate these risks. In addition to that, any deficiency in outsourcing may cause reputation risk, legal risk, compliance risk or strategic risk. Ultimately it would affect the profitability of FIs.

5. Prevailing IT Supervisory Framework and Regulation

Figure 7
Prevailing IT Supervisory Framework and Regulation

No.	Item	Yes/No
1	Is IT Implementation reported regularly?	Yes
2	Is IT audit conducted?	Yes
	By bank/IT supervisors from supervisory authority	Yes
	Off-site	
	On-site	Yes
	By internal or external (third party) auditors (on-site)	Yes
	Special IT audit/examination outside regular examination (on-site)	
3	Does the formal framework exist?	Yes
4	If yes, is it stipulated in a regulation?	Yes
5	Is there minimum requirement in IT Implementation?	
	Are the following items implemented: Active supervision by Top Management (IT Steering Committee)	Yes
	IT Policy and Standard Operating Procedure	Yes
	IT risk is included in the risk-based management	Yes
	System development life cycle	Yes
	All layers of IT system	Yes
	Internal control system for IT Implementation	Yes
	Business Continuity Plan and Disaster Recovery Plan	Yes
	Periodical IT audit (internal/external)	Yes
6	Because it involves supervision procedure, is IT outsourcing especially regulated?	Yes
7	Because it involves consumer protection, is E-banking products especially regulated?	Yes
8	Are any IT-related laws (cyber law, e-commerce, m-commerce, digital signature) installed?	Yes

No.	Item	Yes/No
1	Is it conducted regularly?	Yes
2	If not regularly, is it conducted case by case?	
3	If regularly, objects of audit:	
	Organisation and Management	Yes
	System development process	Yes
	Operation	Yes
	Software and Application, including e-Banking	Yes
	Security (authentication, authorisation and protection – including audit trails, encryption)	Yes
	BCP/DRP	Yes
	Communication Network	Yes
	Outsourcing process	Yes
	Internal Auditing	Yes

5.1 Information Systems Audit

The Bank Supervision Department of the Central Bank of Sri Lanka conducts Information Systems (IS) audit based on its own supervisory framework. The scope of the examination is classified under six categories namely:

- Management
- Environment and Physical Control
- Logical access control
- Software review
- Backup, recovery and contingency planning
- Documentation

5.2 Information Systems Audit Procedure

5.2.1 Management

- Review the IT policy of the Bank. Check whether the management has set up a special board committee for IT related activities. (The Corporate Governance Direction issued by the Central Bank of Sri Lanka requires the members of the Board of Directors of all commercial banks to be able to abreast with the IT challenges.)

- Review committee minutes to ascertain the approach of the IT strategy of the Bank and the knowledge of the committee members to align IT strategies with business promotions.
- Check the compliance with all applicable laws, rules and regulations relating to IT functions of the Bank.
- Check the adequacy of the qualifications of the IT staff and training policy.
- Determine the IT security of the Bank with special attention to responsibility allocation, segregation of duties, job rotations, access controls to the database.
- Ensure that the Bank has entered into agreements for all maintenance work appropriately.
- Review the steps taken by the management to rectify the deficiencies observed by the previous examinations and audits.

5.2.2 Environment and Physical Controls

- Check the physical location of the computer installation to ensure that it is safe from potential hazards, such as water seepages, fire, and the like.
- Check the physical access controls of the CPU room.
- Make sure that the fire alarms and smoke detection system have been installed and in working condition. The staff should be educated on usage.
- Ensure that an adequate distance has been maintained between UPS and CPU room. Extra batteries for UPS are to be kept outside the computer cabin.
- Register to be maintained for servicing and maintenance of UPS, CPU and batteries.
- Check the availability of a generator with adequate capacity to cover the computer peripherals and the AC of the CPU room.
- Ensure that the Bank has obtained Insurance coverage for all IT assets.
- Check whether all computers and peripherals are recorded in the assets register and all items are verified periodically.

5.2.3 Logical Access Control

- Check the user profile to satisfy that all users listed in the system are to be working in the Bank and the users who have been transferred, retired or resigned are to be deleted from the system.
- Check the procedure for issuing and controlling over passwords to the staff.
- Make sure that the users are provided with the option to change the password.
- The user ID's are to be unique and should be identified with specific user in the bank and used for recording the activity done by that particular user.
- Check whether the management of the bank has obtained an undertaking and acknowledgement from all system users for the acceptance of the password.
- The system should ensure that the password validity period for each user is restricted to the authorised duration. Periodic change of password should be mandatory.
- The root password of operating system software and database software are to be enclosed in a sealed envelope and kept in a safe custody under high-level supervision.
- Check whether the standard anti-virus software is to be installed in all PC's.
- Check the implementation of parameters for all the master tables and the policy over the change of parameters.
- Access to parameters in the system should be restricted and make sure that only authorised officers are permitted to change parameters.
- All parameter values of existing accounts are to be printed and checked to ensure that they are set properly.
- Check whether all changes to the parameters are lodged in audit trials.

5.2.4 Software Review

- Uniformity of software across all branches of the bank.
- Make sure that all the software versions have been licensed.
- Only approved software approved by IT department should be installed and used at all offices.
- Check the effectiveness of the software package with the special attention to the adequacy of the MIS for regulatory reporting, user friendliness, coverage of all banking activities, etc.

5.2.5 Backup, Recovery and Contingency Planning

- The backup procedure.
- The backup procedure of the bank should be documented and communicated to all operational staff of the Bank.
- The system administrator should be made responsible for daily backups.
- The backup should be stored both onsite and offsite locations.
- The system backups are to be kept in fireproof cabinets and tested periodically.

5.2.6 Documentation

- Make sure that the management posses all documents relating to system developments and kept in a fireproof cabinet under dual control.
- All user manuals of hardware and software are to be documented and kept in a safe custody.
- Check whether exceptional reports are generated by the system and are properly attended to.
- Make sure that all the reports are chronologically filed and kept in a safe custody for future reference.

6. Issues and Challenges

6.1 Issues

- In Sri Lanka the minimum requirements for IT implementation are not specified. Therefore it is required to enforce IT implementation standards for FIs.
- Lack of attention of the senior management over IT-related issues.
- Under utilisation of IT resources.
- Absence of tested Business Continuity Plan (BCP).
- Inadequate level of awareness among the staff of FIs' on IT-related risks.
- Increase IT-related frauds.

6.2 Challenges

- Difficulties faced by some small banks to incur expenditure to enhance their IT infrastructure.
- To bring all banks into common payment system.
- Frauds and lapses in internal control system due to negligence.
- High cost of customisation.

7. Policy Recommendations

1. It is suggested to appoint at least one member of the Board of Directors with competence and skills in Information Technology.
2. It is recommended to appoint a board committee to monitor the IT function of the FI. It is required to meet the committee in a frequent manner to monitor and evaluate IT performance with special emphasis on the adequacy of internal control systems.
3. The management should provide an assurance to the supervisory authority confirming that:
   - All user requirements and specifications are addressed by the Information System (IS).
   - IS is in compliance with all existing Laws and Regulations.
   - A tested BCP has been set up.
   - Necessary steps have been taken to protect and retain all data and information for a minimum period specified by the regulator for future reference.
4. It is recommended to obtain an independent assurance about the compliance of the IS with the laws and regulations, internal control procedures and generally accepted procedures.

CHAPTER 9

THE SUPERVISORY IMPACT OF TECHNOLOGY ON SEACEN FINANCIAL INSTITUTIONS: ISSUES AND CHALLENGES IN TAIWAN

by Yi-Chang Lee[1]

1. Introduction

1.1 Background and Objectives

Technology has played a major part in the broadening and deepening of the financial markets. Financial institutions implement technology to reduce the cost of operation as well as provide better services. IT has become an integral part of banking operations.

The technological transformation of the banking sector presents unique challenges to bank supervisors. It not only requires the creation of new supervisory tools for many newly developed areas such as e-banking, but also the evolving banking technology and its inherent risks can render the prevailing supervisory framework obsolete and inadequate rapidly. Bank supervisors, therefore, must continually strive to keep up with the changing technology-driven environment to harness new technology in their effort to ensure a safe and sound banking system.

In light of the above and the need to increase the awareness of IT supervision for financial institutions, SEACEN established this collaborative research project with the following objectives:

- To assess banks' financial risks in relation to the payment and settlement systems and overall financial stability;
- To examine country experiences with regard to the supervisory impact of technology; and
- To develop the research output into a case study relevant to SEACEN training courses.

---

1 Author is Senior Auditor of the Department of Financial Inspection of Central Bank of the Republic of China (Taiwan). The views and opinions expressed in this paper do not represent the policy or stance of Central Bank of the Republic of China (Taiwan).

1.2 Summary

There are 388 banking institutions in Taiwan. The usage of IT is unavoidable in the banking sector. The applications of IT in these banking institutions can be classified into three categories:

- Category A: This category covers the computerisation of the core business of the banking institutions, such as deposits, loans, foreign exchange, treasury, trustee, credit cards, remittance, ATM, etc. Almost all the banking institutions in Taiwan are in this category.
- Category B: This category encompasses e-Banking and covers the banking products and services that are distributed through electronic channels. Continuous technological innovation and competition among the existing banks have spurred the rapid development of e-banking over the last decade. It is apparent that Internet banking has emerged as the master stream. Today all the domestic banks are engaging in Internet banking.
- Category C: This category consists of Management Information Systems (MIS) that are implemented by banks to improve the quality of their management in the face of keen competition. The MIS are implemented in the areas of Asset and Liability Management, Risks Management, Performance Management and Data Warehousing.

The major risk in IT implementation is operational risk. This is in spite of the advancement of IT usage in the banking industry. IT-related incidences in Taiwan's domestic banking sector reveal that most of the risks in IT implementation manifest from improper strategy, improper design, improper management, improper operation, and criminal acts.

The board and senior management of the banking institutions should be responsible for identifying, managing and monitoring the risks in IT implementation. The banking and financial institution supervisors face a rapidly changing landscape in the aspects of technology and customer service innovation, and it is essential for them to stay abreast of the developments and continually enlarge and upgrade their capacity and competencies. Banks are experiencing competitive pressure to roll out new business applications in very compressed time frames. The competition intensifies the supervisory and management challenge to ensure that adequate risk assessments and security reviews are properly carried out prior to the implementation of the new applications.

As Internet banking provides low cost, convenient and efficient services to customers, banks continue to promote products and services via the Internet. As the Internet threats grow rapidly, security consideration becomes an issue of major concern. The customers of Internet banking have the responsibility to manage and

secure their own computing environment, but most of them lack the knowledge and technical know-how to safeguard themselves against malevolent intruders. The supervisory authorities should be concerned with the coverage of the security measures provided by banks to protect customer privacy.

Technically, the system architecture of Internet banking consists of bank server systems, Internet connection and customer-computing environment. Customers play an important role in maintaining a secure e-banking operating environment. While the behavior and conduct of the customers do not fall under the purview of the supervisory authority, they do have an impact on the banking system.

The measures taken by banks today are too passive for them to reap the benefits of Internet banking. Eventually the Internet will enter the main stream of human life. In the development of Internet banking, the challenge to the banks is that they should constructively address and resolve the obstacles and security issues faced by customers in using the Internet services.

2. Overview of the Banking Institutions in Taiwan

The banking institutions in Taiwan include 39 domestic banks, one trust and investment company, 27 credit cooperatives, 289 credit departments of farmer's and fishermen's associations, and 32 local branches of foreign banks. The total number of branches reached 5,836 as at the end of June 2008.

Table 1
Number of Banks and Branches

Categories of Banking Institutions	HeadOffice	Branches
Domestic banks	39	4,556
Trust & investment Co.	1	6
Credit cooperatives	27	270
Credit department of farmers' & fishermen's associations	289	852
Local branches of foreign banks	32	152
Total	388	5,836

Source: Financial Statistics Monthly at the end of June 2008

Domestic banks are relatively large in terms of their assets. They accounted for 85.6% of total assets of banking institutions as at the end of June 2008. The asset share of the banking institutions are shown in Table 2.

Table 2
Assets of the Banking Institutions in Billion of NT$

Categories of Banking Institutions	Assets	Share of Total Assets
Domestic banks	30,589	85.6%
Trust & investment Co.	15	0.1%
Credit cooperatives	596	1.7%
Credit department of farmers' & fishermen's associations	1,516	4.2%
Local branches of foreign banks	3,004	8.4%
Total	35,720	100.0%

Source: Financial Statistics Monthly at the end of June 2008

2.1 Condition and Performance of Domestic Banks

2.1.1 Major Income Components

The sector's net income (excluding interest) before tax in the first quarter of 2008 grew dramatically compared with the same period of 2007. The major income components are tabulated as follows.

Table 3
Major Income Components

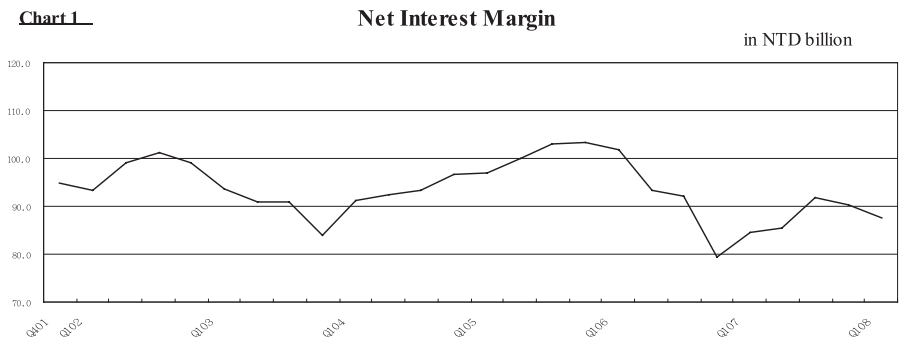
			NT$ billion
	Jan.-Mar. 2007	Jan.-Mar. 2008	% Change
Income			
Net interest income	84.7	87.6	3.4
Net revenues other than interest	8.0	39.6	395.0
Expense			
Loan loss provision	31.0	25.3	-18.4
Other expense	66.3	74.8	12.8
Net income	-4.6	27.0	-

Source: Condition and Performance of Domestic Banks at First Quarter's End 2008 Central Bank of the Republic of China (Taiwan)

2.1.2 Net Interest Margin (NIM)

The NIM was NT$ 87.6 billion during this quarter, slightly decreasing by NT$ 2.7 billion (-2.99%) compared with the previous quarter (Chart 1).

Chart 1

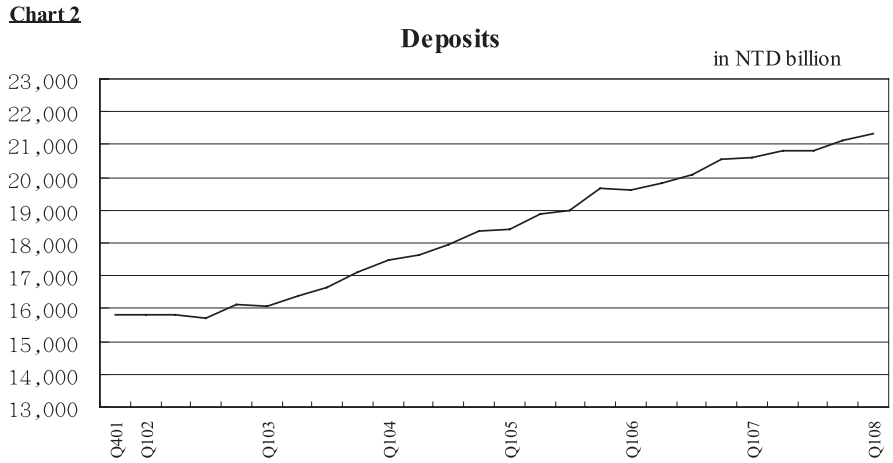


Source : Condition and Performance of Domestic Bank's at First quarter's end 2008 Central Bank of the Republic of China (Taiwan)

2.1.3 Deposits

Total deposits as of the first quarter's end of 2008 were NT$21,333.7 billion, increasing by NT$ 197.1 billion compared with the preceding quarter. It was mainly due to the increase in time deposits. The annual growth rate of total deposits decreased 3.23 percentage points from 7.36% as at the end of the first quarter of 2007 (Chart 2).

Chart 2

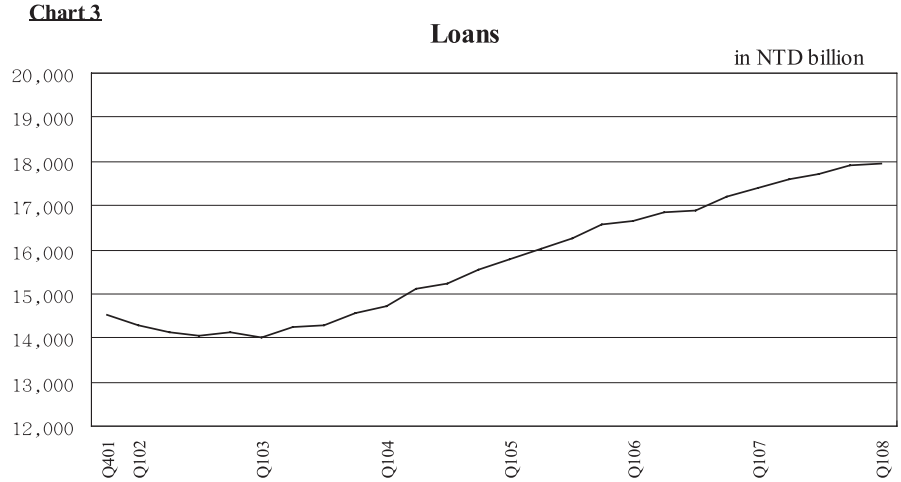


Source : Condition and Performance of Domestic Bank's at First quarter's end 2008 Central Bank of the Republic of China (Taiwan)

2.1.4 Loans

The total loans were NT$ 17,958.0 billion as at the end of the current quarter, increasing by NT$ 42.9 billion (0.24%) compared with preceding quarter. The annual growth rate was 2.18%, decreasing 4.78 percentage points from 6.96% as of the same period of 2007. The trend was mainly due to a slowdown of bank claims on government and private sectors (Chart 3).

Chart 3

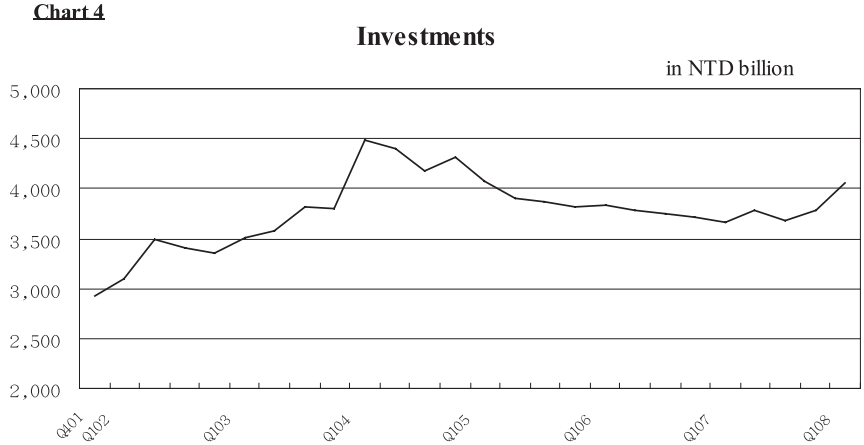


Source : Condition and Performance of Domestic Banks at First quarter's end 2008
Central Bank of the Republic of China(Taiwan)

2.1.5 Investments

The total investments amounted to NT$4,049.3 billion, increasing by NT$ 269.5 billion (7.13%) compared with the previous quarter, mainly due to the increased purchase of Negotiable Certificate of Deposits (NCDs) issued by CBC (Chart 4).

Chart 4

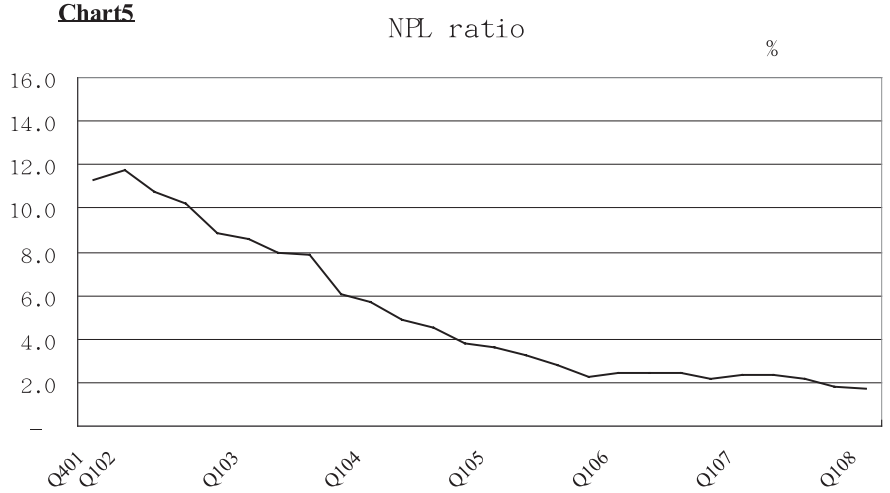


Source : Condition and Performance of Domestic Banks at First quarter's end 2008
Central Bank of the Republic of China(Taiwan)

2.1.6 Asset Quality

The average NPL ratio at the end of this quarter went down by 0.15 percentage points to 1.68% from previous quarter. Along with the efforts to enhance risk management, the asset quality of the overall banking sector remains healthy. The average provision coverage ratio was 72.32%, 4.32 percentage points up from 67.0% as at the end of the previous quarter. The sector's average provision coverage ratio stayed on an upward trend strengthening in the capacity capacity of risk management (Chart 5).

Chart5

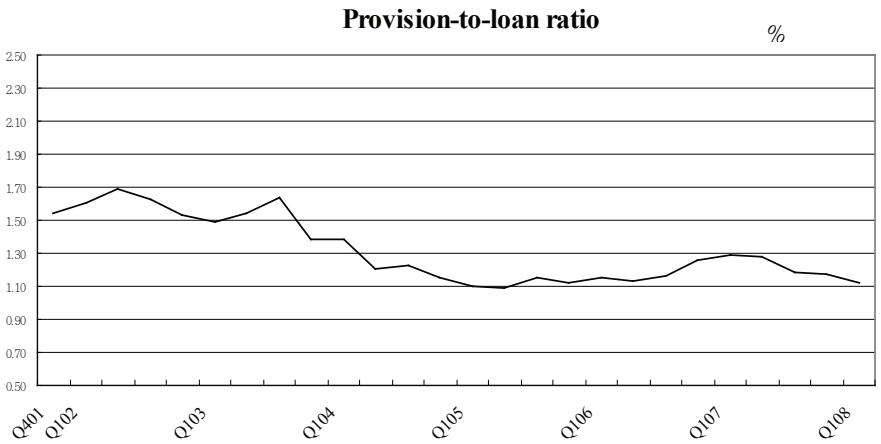


Source : Condition and Performance of Domestic Banks at First quarter's end 2008
Central Bank of the Republic of China(Taiwan)

2.1.7 Provision-to-Loan Ratio

The provision-to-loan ratio was 1.13%as at the end of the current quarter, slightly leveling off from 1.17%as of the preceding quarter. It was due to the slight decrease of loan loss provisions and increase of loans, reflecting the banking sector's optimistic attitude in loan policy (Chart 6).

Chart 6

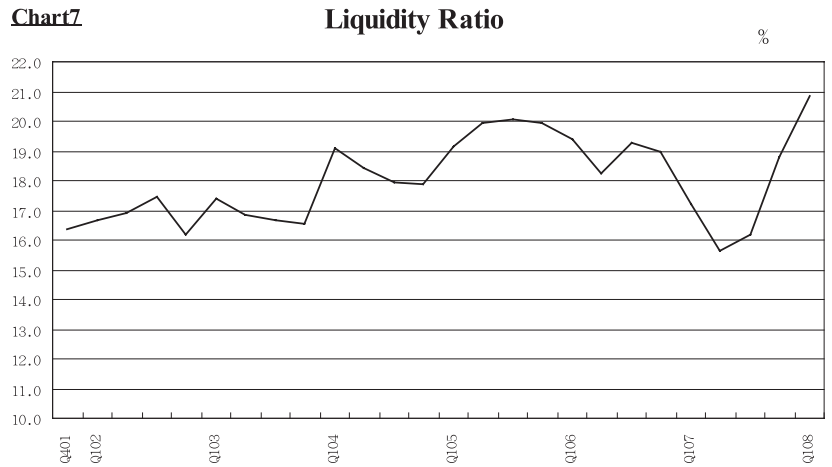


Source : Condition and Performance of Domestic Banks at First quarter's end 2008
Central Bank of the Republic of China(Taiwan)

2.1.8 Liquidity Ratio

The liquidity ratios of all the domestic banks exceed the statutory minimum ratio (7%) in March 2008. The average liquidity ratio was 20.86%, increasing by 2.08 percentage points from 18.78% in December 2007. Overall, the domestic banking sector had ample liquidity. All the data was in terms of the average of the last month of quarters (Chart 7).

Chart7



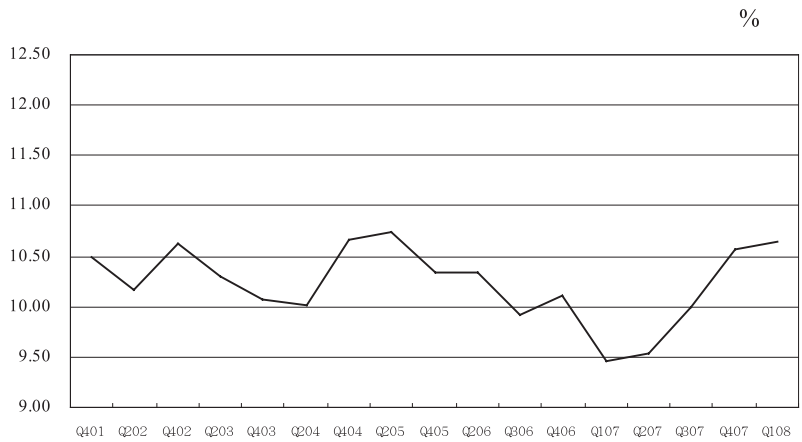
Source : Condition and Performance of Domestic Banks at First quarter's end 2008
Central Bank of the Republic of China(Taiwan)

2.1.9 Capital Adequacy Ratio

The average BIS capital adequacy ratio was 10.64% as at the end of March 2008, increasing by 0.07 percentage points from 10.57% as at the end of December 2007. Taken as a whole, most of the domestic banks have adequate capital. The average capital adequacy ratio has been published quarterly since the third quarter of 2006. The data disclosed was based on unaudited reports (Chart 8).

Chart 8

Capital Adequacy Ratio



Source : Condition and Performance of Domestic Banks at First quarter's end 2008
Central Bank of the Republic of China(Taiwan)

2.2 ATM and Credit Card

In Taiwan, ATMs (Automated Teller Machines) provide round-the- clock service, seven days a week. Customers of banks can use a financial card at any ATM machine with the mark of the Financial Information Service Co., Ltd ("FISC") to make interbank withdrawals, account transfers, bill payments, tax payments, and balance inquiries. They can use VISA or MasterCard credit cards at any ATM machine with the "VISA" or "MASTERCARD" marks to take a cash advance. They also can use VISA or MasterCard debit cards at any ATM with the "*Plus*" or "*Cirrus*" logo to make cross-border cash withdrawals in the local currency. The ATM statistics are shown in Table 4.

Table 4
ATM Statistics

End of Period	No. of ATM installed	ATM card Issued (in 1000)	Circulated ATM card (in 1000)	Count of Transactions (in 1000)	Amount of Transactions (in million NT$)
1994	8,528	26,164	19,769	257,751	2,894,272
1995	9,536	32,512	23,658	308,061	3,498,559
1996	10,459	38,893	27,986	356,021	4,044,204
1997	11,296	46,100	32,563	398,265	4,801,748
1998	12,633	53,930	36,781	427,326	5,186,950
1999	13,683	61,639	41,698	475,666	5,882,658
2000	14,894	70,524	47,512	525,610	6,729,964
2001	15,951	79,116	53,249	539,301	6,377,504
2002	16,787	87,548	58,368	566,911	6,909,313
2003	19,097	96,898	63,760	610,372	7,180,615
2004	21,449	113,592	68,247	688,879	8,469,841
2005	24,212	130,297	73,372	727,235	9,073,712
2006	24,783	136,298	71,905	727,020	8,749,668
2007	25,121	145,178	74,252	751,266	9,440,966
2008					
Jan.	25,019	142,183	72,904	68 053	930,398
Feb.	24,989	141,070	72,678	58 325	888,881
Mar.	25,138	140,047	72,457	64 718	905,890
Apr.	25,271	140,601	72,781	62 840	926,051
May.	25,402	141,207	73,127	64 210	953,673
Jun.	25,461	141,816	73,322	63 380	980,495

Source: Financial Supervisory Commission, Executive Yuan, R.O.C

The largest credit card networks in Taiwan are Visa and MasterCard. The National Credit Card Center also provides credit cards that are only available in Taiwan. The credit card statistics are shown in Table 5.

Table 5
Credit Card Statistics

End of Period	Circulated Credit Cards (in 1000)	Amount of Credit Card Transactions (in million NT$)		
		Total Tran.	Local Tran.	Overseas Tran.
1994	2,709	131,553	—	—
1995	3,676	190,653	—	—
1996	5,467	272,387	227,386	45,001
1997	7,665	374,425	322,480	51,945
1998	10,640	491,097	441,505	49,592
1999	13,575	597,786	545,830	51,956
2000	18,276	719,770	660,934	58,836
2001	24,135	771,861	716,162	55,699
2002	31,591	873,599	813,492	60,107
2003	37,850	998,885	941,637	57,248
2004	44,182	1,254,482	1,177,015	77,467
2005	45,494	1,420,984	1,341,336	79,648
2006	38,324	1,380,462	1,299,164	81,298
2007	36,437	1,413,455	1,329,901	83,554
2008				
Jan.	36,163	129,524	122,678	6,845
Feb.	35,988	109,103	103,110	5,993
Mar.	35,947	106,360	99,848	6,512
Apr.	35,723	112,181	105,260	6,921
May.	35,576	113,625	106,697	6,928
Jun.	35,446	134,505	127,809	6,696

Source : Financial Supervisory Commission, Executive Yuan, R.O.C

3. Survey of IT Implementation

3.1 The Development of Technology Infrastructure

3.1.1 Communication & Internet

Chunghwa Telecom is the major provider for communication infrastructure in Taiwan. It provides the following communication facilities:

- Leased Line
- Dedicated Line
- Broadband Networks
  - ADSL
  - DSL
- ATM (Asynchronous Transfer Mode) Service
- Frame Relay Service
- WLAN Services
- ISDN Dial-up
- FTTx (which includes all fiber technologies from fiber-to-the-kerb to fiber-to-the-home, such as FTTN, FTTC, FTTB and FTTH)
- Satellite (iDirect VSAT satellite and mesh networks rental services)

The results of the 2007 survey of the current state of demand for broadband, mobile and wireless applications among Taiwanese households, conducted by the Institute of Information Industry and sponsored by the Industrial Development Bureau of the Ministry of Economic Affairs, reveal that, as of August 2007, 79% of households in Taiwan own computers; 71% of households have Internet access; 69% of households have broadband access and 96% of online households are using broadband connections.

The statistics released by the National Communications Commission (NCC) indicate that there were a total of 24.3 million mobile phone subscribers (including 2G, 3G and PHS) in Taiwan as of December 2007. This represents an increase of approximately 660,000 subscribers or 2.8% compared with the first half of 2007. The mobile phone penetration rate had climbed up to 106%, 3% higher than the first half-year. Table 6 shows the communication infrastructures installed in Taiwan.

Table 6
Communication Infrastructures Installed in Taiwan

No.	Item	Yes/No
1	Communication Network	
	Cable (Phone line)	Yes
	Satellite	Yes
	Fiber Optic	Yes
2	Use of Cellular Phone	
	Is it relatively wide spread?	Yes
3	Use of Internet	
	Is it relatively wide spread?	Yes

Source: Survey of this research project

3.1.2 Payment Systems

There are five major payment systems in Taiwan:

- CBC Interbank Funds Transfer System

  The CBC Interbank Funds Transfer System (CIFS) was established in 1995. It is operated and governed by the Central Bank of the Republic of China (Taiwan), hereafter referred as the CBC. The participants of the CIFS comprise banks, investment and trust companies, and bills finance companies. The banking and financial institutions which maintain transaction accounts with the CBC may directly use the CIFS to transfer funds. Payment instructions are also sent over the CIFS for settling obligations on cheque clearing, adjusting reserve account balances, or making payments associated with interbank loans, bill/bond transactions.

  Previously, the CIFS is operated a dual system of designated-time netting and real-time gross settlements. To minimise settlement risk, the CBC abolished designated-time settlements in September 2002. That is, the CIFS is embedded with real-time gross settlement (RTGS) function. Payments are processed through the CIFS individually and continuously during the day in real time.

- Interbank Remittance System

  The Interbank Remittance System (IRS), launched in August 1987, is operated by the FISC. The IRS provides remittance services to the general public, government agencies, and banks.

- Credit Card and Shared ATM System

  The largest credit card networks in Taiwan are Visa and MasterCard. The interbank settlements of credit card transactions between card-issuing banks and the retail merchants' banks are made by the FISC, or the National Credit Card Center.

  The Shared ATM System is operated by the FISC. All the participants in the IRS can join the Shared ATM System to provide 24-hour service transactions with regard to cross-bank withdrawal, balance inquiry, funds transfer, credit card cash advance, and IC card loading. Net positions are settled daily through a special account maintained at the CBC.

- Clearing House System

  The CBC supervises the Taiwan Clearing House System which handles clearing and settlement of cheques, promissory notes, and drafts among banks. All banks in Taiwan using these facilities are required to open reserve accounts at the CBC where the net settlement balances will be debited or credited to these accounts. The head office of the Taiwan Clearing House System is located in Taipei and it has 15 local clearing houses outside the Taipei area.

  The participants of the system include banks, credit cooperative associations, credit departments of farmers' associations and fishermen's associations. The CBC is also one of the participants in the Taiwan Clearing House System.

- Central Government Securities Settlement System

  Since the introduction of the Central Government Securities Settlement System (CGSS) in September 1997, central government bonds have been issued in the book-entry form. In October 2001, treasury bills were added to the system and have been issued in the book-entry form since then. The CGSS is a real-time gross settlement system (RTGS) for the issuance, transfer, redemption, and interest payment of central government bonds in the form of accounting entries on computer records.

The ownership of book-entry central government securities is recorded in a two-tier system of accounts. Only the clearing banks are eligible to have book-entry bond accounts and fund accounts (also serve as reserve balances) directly with the Treasury Department of the CBC. All other individuals or entities are required to hold such accounts with the clearing banks.

Currently, book-entry transactions within a clearing bank can be made on a delivery-versus-payment (DVP) basis while those between clearing banks cannot. To reduce the settlement risk in interbank transactions, the CBC plans to link the CGSS with the CIFS to allow clearing banks to handle related settlements on DVP basis. Table 7 shows the information of payment systems in Taiwan.

Table 7
Information of Payment Systems in Taiwan

No.	Item	Yes/No
1	National Payment System	
	Operated by government agency / central bank	Yes
	Operated by an independent or private company	Yes
2	Automated/Computerised Payment System	Yes
3	RTGS	Yes
4	National Securities Settlement System	
	Operated by government agency / central bank	Yes
	Automated/Computerised Settlement System	Yes

Source : Survey of this research project

3.2 The Presence of Technology-supported Financial Products and Services

Banks are highly competitive in Taiwan. All the domestic banks provide Internet Banking service, including WebATM which provides ATM services (except cash withdraw) via the Internet. Table 8 shows the presence of technology-supported financial products and services in Taiwan.

Table 8
Technology-supported Financial Products and Services

No.	Item	Yes/No
1	Credit Card	
	National (only used in the country)	Yes
	International	Yes
2	Debit Card	
	National (only used in the country)	Yes
	International	Yes
3	ATM	
	Individual bank	Yes
	Nationally-Shared ATM	Yes
	Internationally-Shared ATM	Yes
4	Electronic Fund Transfer (EFT)	Yes
5	EFT at Point of Sale	
	National (only within the country)	Yes
	International	Yes
6	Remittance Service	
	Domestic companies	Yes
	International companies	Yes
7	Phone Banking	
	Informational	Yes
	Transactional intra bank	Yes
	Transactional inter bank	Yes
8	Mobile/SMS Banking	
	Informational	Yes
	Transactional intra bank	Yes
	Transactional inter bank	Yes
9	Internet Banking	
	Informational	Yes
	Transactional intra bank	Yes
	Transactional inter bank	Yes
10	Pre-paid card	Yes

Source: Survey of this research project

3.3 The Heterogeneity/Homogeneity of the Technology Implemented in the Financial Institutions.

In the 1970's, most of the banks in Taiwan began to develop IT-related applications. With the encouragement of the relevant authorities, all the domestic banks set up their core banking systems in the 1980's, operating mainly in the deposit and loan business of the banks.

In 1986, the Financial Information Service Co., Ltd (FISC) introduced Cross-Bank Systems, which provide Cross-Bank shared ATM and Cross-Bank remittance service. Banks had to develop their own cross-bank systems to provide these services to their customers. The banks joined the Cross-Bank network gradually. Finally, all the banking institutions including the credit departments of farmers' and fishermen's associations took part in the network. This is an important milestone in the development of payment infrastructure for convenient and automatic banking services in Taiwan.

The relevant authorities encourage the banks to computerise their core business. As a result, banking business in the areas of deposit, loan, foreign exchange, credit cards, investments, trustee, securitisation, derivative and structure products are all supported by technologies.

To further improve management capability and to comply with Basel II, banks also develop technologies to support various types of risk management, such as credit risk, market risk, operational risk, asset and liability management, etc.

Table 9 shows the requested survey regarding the implementation of IT-related applications in addition to IT-related products.

Table 9
Implementation of IT-related Applications

No.	Item	Yes/No
1	Core Banking: General Ledger, Third Party Fund, Loan, and Consumer Information File	Yes
2	Treasury	Yes
3	Remittance	Yes
4	Trade Finance	Yes
5	Corporate Online Service	Yes

Source: Survey of this research project

3.3.1 Heterogeneity

- The banking institutions use different platforms to implement technologies and adopt different security management policies and procedures. It is not easy to impose a common security standard for different platforms, and that certainly increases the difficulty in supervisory tasks. The management of banks should be responsible for monitoring the adequacy in security control.

- Commercial banks are highly competitive. They develop technologies to provide state-of-the-art services to customers, while limited-sized banks still adopt technology as automatic calculator.

3.3.2 Homogeneity

- Most of the domestic banks develop technologies on their own to support their core business. The core business context supported by technologies has close similarities.

- Almost all the domestic banks adopt centralised architecture to implement technologies.

4. Impact of IT Implementation on Financial Institutions

4.1 Risks Assessment

The usage of IT is unavoidable in the banking sector. The banking institutions in Taiwan require IT support for them to increase efficiency, provide better services, obtain better profits and compete for markets. The implementation of IT applications by the banking institutions in Taiwan can be classified into three categories:

Table 10
Categories of IT Implementation in Banking Institutions

Category	Scope of IT Implementation
Category A	Core Banking
Category B	e-Banking
Category C	Management Information System

Source: Survey of this research project

Category A: Core Banking covers the computerisation of the core business of the banking institutions, such as deposit, loan, foreign exchange, treasury, trustee, credit cards, remittance, ATM, etc. Most of the banking institutions in Taiwan fall under this category.

Category B: e-Banking collectively covers the banking products and services that are distributed through electronic channels, such as Phone Banking, Home Banking, Firm Banking, Mobile Banking, Internet Banking, etc. Continuous technological innovation and competition among the existing banks have spurred the rapid development of e-Banking over the last decade. It is apparent that Internet Banking has emerged as the master stream. All domestic banks are engaging in Internet banking.

Category C: This category consists of Management Information Systems (MIS) that are implemented by banks to improve the quality of their management especially in the areas of Asset and Liability Management, Risks Management, Performance Management and Data Warehousing.

The usage of IT carries risks for all industries, especially so for the financial industry. The implementation of IT applications not only broadens and deepens the financial institutions, but it can also influence the stability of the whole financial system.

4.1.1 General Risks

The major risk in IT implementation is operational risk. This is in spite of the advancement of IT usage in the banking industry. From a review of all the IT-related incidents in the domestic banks of Taiwan, we find that most risks in IT implementation are due to improper strategy, improper design, improper management, improper operation, and criminal acts. In general, we assess risks from the security objectives of IT implementation:

- Integrity: When data is incomplete or inaccurate, it may cause Operational Risk, Strategic Risk, Reputation Risk, Legal Risk and Compliance Risk.

- Confidentiality: When information is not protected or there is unauthorised access to the system, it may cause Operational Risk, Reputation Risk, Legal Risk and Compliance Risk.

- Availability: When the system is not available for use, it may cause Operational Risk, Reputation Risk, Strategic Risk and Compliance Risk.

- Effectiveness & Efficiency: When the system does not deliver an expected function or cause a sub-optimal use of resource, it may cause Operational Risk.

4.1.2 Specific Risks

An IT system that is implemented to support the management of specific risks, such as Liquidity Risk and Credit Risk, may actually bring about the specific risks, if the IT system does not function according to its design, as planned.

4.2 Risks and Impact of IT Usage on Supervisory Practices

Table 11 shows the risks that need to be addressed and controlled in the financial system.

Table 11
IT-related Risks in Financial System

No.	Item	Yes/No
1	Operational Risk	Yes
2	Liquidity Risk	Yes
3	Credit Risk	Yes
4	Strategic Risk	Yes
5	Reputation Risk	Yes
6	Legal Risk	Yes
7	Compliance Risk	Yes

Source: Survey of this research project

Currently, the banking institutions in Taiwan do not have any quantitative approach in measuring the risks in IT implementation. As is generally acknowledged, the board and senior management of the banking institution should be responsible for identifying, managing and monitoring the risks in IT implementation. They should establish proper procedures to ensure that the risks are assessed and are adequately managed, and that the banking operations are compliant with the regulations.

In Taiwan, the banking institutions are required to acquire the approval of the relevant authorities before introducing a brand-new product or service to their customers, especially a product or service with technological innovation. The relevant authorities are tasked to ensure that the risks are adequately assessed and the management plans are in place to mitigate the risks, before approval is given for the launching of a brand-new product or service.

The banking and financial supervisors face a rapidly changing banking environment as banks innovate with IT technology to compete in the marketplace. It is essential for them to keep abreast of the developments and continually enlarge and upgrade their capacity and competencies. Banks are experiencing competitive pressure to roll out new business applications in very compressed time frames. The competition intensifies the supervisory and management challenge to ensure that adequate risk assessments and security reviews are conducted prior to implementing new applications.

5. The Prevailing IT Supervisory Framework and Regulations

5.1 Principles

In order to ensure the stability and safety of the financial markets, the following principles are adopted in all aspects of supervision (including IT supervision):

- To maintain the soundness of the banking system with a liberal and predictable legal environment;
- To protect the interest of depositors;
- To develop the banking sector and enhance its market competitiveness; and
- To establish a financial management system in line with international norms and standards.

5.2 Regulatory Framework and Regulations

5.2.1 Legal Framework

The Banking Law, Financial Holding Company Law, Securities & Futures Law, and Insurance Law are the main pillars of the legal framework for the domestic financial market. In addition, there is a separate Offshore Banking Act that governs offshore banking units and the Law governing Credit Cooperatives which regulates community financial institutions.

To improve the legal framework and prevent technology-related crimes, new legislations have been developed to reinforce the foundation of the legal system of Taiwan, such as Criminal Law, Consumer Protection Law, Money Laundering Control Act, Data Protection Law, Electronic Signature Law, etc.

5.2.2 Regulatory Agencies

- Financial Supervisory Commission

  Pursuant to the Regulation Governing the Establishment and Organisation of the Financial Supervisory Commission of the Executive Yuan, enacted on 10 July 2003, the Financial Supervisory Commission (FSC) was inaugurated and commenced operation on 1 July 2004. The authority of financial supervision was shifted from the Ministry of Finance (MOF) to the FSC since then.

The primary function of the Commission is to consolidate the supervision and examination of the banking, securities and futures, insurance as well as the financial holding companies under one supervisory authority with greater independent power. The FSC functions as an independent agency that directly reports to the Executive Yuan. Its responsibilities include supervision, examination, and inspection of the financial market.

- The Central Bank of the Republic of China (Taiwan)

  The Banking Law and the Law Governing the Central Bank of the Republic of China mandates the Central Bank of the Republic of China (CBC) to implement monetary policy and foreign exchange regulations. The CBC adjusts the national money supply to promote its policy goals of price stability and sound economic growth. The CBC is also concerned with the sound operation of banks and exchange rate stability.

  Since the FSC was set up on 1st July 2004, the CBC stopped carrying out regular full-scope on-site examinations of individual financial institutions. To facilitate the implementation of the Central Bank's policies, the Bank retains the authority to carry out target examinations on issues related to monetary, credit and foreign exchange policies and payment system. In addition to on-site target examinations, the Bank implements off-site monitoring to identify the weaknesses of individual financial institutions and to grasp the whole picture of the financial system in order to respond appropriately in a timely manner.

- Bureau of Agricultural Finance (BOAF), Council of Agriculture

  The BOAF is responsible for supervising agricultural finance institutions, including the credit departments of farmers' and fishermen's associations.

5.2.3 Regulations

In addition to the laws legislated to prevent technology-related crimes, the major regulations applied in technology supervision are as follows:

- Rules Governing Information Security Management of Executive Yuan and Organisations under the Yuan;
- Implementation Rules for Internal Audit and Internal Control System;
- Information System Security Standards for Financial Institution;
- Risk Management Principles for Electronic Banking; and
- Guidelines for Security Measures of Financial Institutions for Electronic Banking Services.

Table 12
IT Supervisory Framework

No.	Item	Yes/No
1	Is IT Implementation reported regularly?	No
2	Is IT audit conducted?	Yes
	By bank / IT supervisors from supervisory authority	Yes
	Off-site	No
	On-site	Yes
	By internal or external (third party) auditors (on-site)	Yes
	Special IT audit/examination outside regular examination (on-site)	Yes
3	Does the formal framework exist?	Yes
4	If yes, is it stipulated in a regulation?	Yes
5	Is there minimum requirement in IT Implementation?	Yes
6	Are the following items implemented: Active supervision by Top Management (IT Steering Committee)	Yes
	IT Policy and Standard Operating Procedure	Yes
	IT risk is included in the risk-based management	Yes
	System development life cycle	Yes
	All layers of IT system	Yes
	Internal control system for IT Implementation	Yes
	Business Continuity Plan and Disaster Recovery Plan	Yes
	Periodical IT audit (internal/external)	Yes
5	Because it involves supervision procedure, is IT outsourcing especially regulated?	Yes
6	Because it involves consumer protection, is e-Banking products especially regulated?	Yes
7	Are any IT-related laws (cyber law, e-commerce, m-commerce, digital signature) installed?	Yes

Source: Survey of this research project

5.3 References/Orientation for the Prevailing Supervisory Framework

Prior to the establishment of the FSC, the original authority, the Ministry of Finance (MOF), in addition to its jurisdiction over national treasury, taxation and customs, was in charge of the supervision of Taiwan's financial market through its three major subordinate agencies, namely, the Bureau of Monetary Affairs (BOMA), the Securities and Futures Commission, and the Department of Insurance. Among the agencies, BOMA is responsible for the formulation and implementation of policies and regulations.

The authority for financial supervision was shifted from the Ministry of Finance (MOF) to the Financial Supervisory Commission (FSC) since 1 July 2004. Most of the IT supervisory framework remains unchanged.

5.4 IT Supervisory and Audit Practices

There are three major layers of IT audit that are conducted in the banking institutions of Taiwan:

- Self-audit conducted by the Information Department itself;
- Internal-audit conducted by the Audit Department reporting to the Board of Directors; and
- External-audit conducted by the supervisory authority.

5.4.1 Self-audit

The Information Department of the banking institution is required to conduct self-audits regularly. The Department has the responsibility to help the bank achieve security objectives in its IT implementations. Self-audit is a management approach for the department to conduct reviews to determine if the policies and procedures have been properly complied with.

The findings of the self-audit should be well documented. The Department should conduct full scope self-audits twice a year and carry out targeted self-audits ten times a year. The self-audit activities are monitored by the audit department of the Board of Directors.

5.4.2 Internal Audit

Internal audits are conducted by the Audit Department reporting to the Board of Directors. The Department is required to conduct full-scope internal audit on site at least once a year. It should be conducted by specialised IT auditors, and the audit reports should be submitted to the supervisory authorities.

5.4.3 External Audit

IT examinations are included within regular full-scope on-site examinations conducted by the supervisory authority. The frequency of regular full-scope examination depends on the performance of the banks. The average frequency is once every 12 to 18 months. IT examinations are conducted by specialised IT auditors in accordance with the examination handbooks. Any finding in the examination would be recorded and followed up subsequently.

Table 13
Regarding On-site IT Audit

No.	Item	Yes/No
1	Is it conducted regularly?	Yes
2	If not regularly, is it conducted case by case?	
3	If regularly, objects of audit:	
	Organisation and Management	Yes
	System development process	Yes
	Operation	Yes
	Software and Application, including e-Banking	Yes
	Security (authentication, authorisation and protection – including audit trails, encryption)	Yes
	BCP/DRP	Yes
	Communication Network	Yes
	Outsourcing process	Yes
	Internal Auditing	Yes

Source: Survey of this research project

5.5 Specialised IT Supervisors / Auditors

The Financial Supervisory Commission (FSC) is the sole statutory financial supervisor. The Commission has 17 specialised IT supervisors / auditors.

5.6 Coordination Among the Financial Institution Authorities

Pursuant to the Financial Supervisory Commission Act, there is a coordination mechanism among the financial authorities in place. The "Financial Supervision Coordination Group" which is composed of the senior officers of the FSC, the CBC and other related financial authorities meets every month, and when necessary, to coordinate and cooperate on issues of financial supervision, management and examination.

6 Issues and Challenges

6.1 "What Appropriate Measures have been Taken by the Banks to Ensure Adherence to Customer Privacy Requirements in Internet Banking?"

As Internet banking provides low cost, convenient and efficient services to customers, banks continue to promote products and services via the Internet. At the same time, the Internet threats are also growing rapidly, and security consideration is a major concern in promoting Internet banking.

Most of the banks providing Internet banking services stressed they have instituted these counter-measures:

- Adoption of security measures at the transaction level.
  Banks are using strong encryption supports to ensure message confidentiality, integrity, authentication, non-duplication and non-repudiation.

- Establishment of Security Policies and Operating Guidelines.
  Only authorised persons are allowed access to the systems and audit trails are preserved for any access attempts. Comprehensive security policies and operating guidelines are implemented, enforced and monitored by the management to achieve security objectives.

- Improvement of the reliability of the system.
  To improve the reliability of the computer system, computer systems are kept in operational conditional to provide high usability, and decrease the chances of non-availability.

- Protection of bank's internal systems from malicious attacks.
  Measures have been taken to protect internal computer systems from malicious attacks, such as firewalls, virus detection software, and intruder detection systems, etc.

In March 2004, four commercial banks in Taiwan reported that their customers were infected by the "Trojan Horse" virus. Criminals were using the "Trojan Horse" to steal the passwords of customers that were used to access Internet banking services to transfer out funds in customers' accounts. This event caused a temporary stoppage in non-previously-agreed fund transfers of all the banks. The supervisory authority requested the banks to reassess the risks and the measures in mitigating risks, and that banks are to resume this service with at least 2-factor authentication procedures. This event illustrates the intrusion of customer's privacy in the customer's own computing environment.

Though the customers of Internet banking have the responsibility to manage and secure their own computing environment, most of them lack the knowledge and technical capability. Their computer systems may be infected through the mere browsing of the web pages, or through opening an e-mail. It is glary that most of the bank customers lack the knowledge in technologies to prevent and protect themselves against malevolent intruders. There have been instances of intrusions where the customers might not even have been aware of them.

The Internet has become an important channel for banking business. The supervisory authorities should concern with the coverage of the security measures taken by the banks to protect customer privacy.

6.2 Challenges

"What are the Appropriate Measures that could be Taken by the Bank to Assist their Internet Banking Customers Manage their Own Computing Environments?"

Banks that provide Internet banking services recognise the weakness existing on the customer's side. To mitigate the risks, most of the banks take the following measures:

- Provision of security-related information to their customers.

  The security-related information is provided in the form of booklets when customers apply for the Internet banking service. Most of the information provided is basic and not up to date.

- Having their customers declare in the agreements that they recognise the existence of risks and they have the responsibility of maintaining and securing their own computing environment.

  Technically, the system architecture of Internet banking consists of bank server systems, Internet and customer computing environment. Customers have an important role to play in keeping a secure e-banking operating environment. Their conduct and behavior can have an impact on the banking system even though they do not come under the purview of the banking and financial institution supervisors.

  The measures taken by banks today are too passive for them to reap the benefits of Internet banking. Eventually the Internet will enter the main stream of human life. In the development of Internet banking, the challenge to the banks is that they should address and resolve the

obstacles and security issues faced by customers in using the Internet services.

7. Policy Adoption

The following major IT implementation policies have been adopted by the IT auditors of the Financial Inspection Division, Central Bank of Republic of China (Taiwan), while IT examinations are conducted of the financial institutions.

- Organic policy
  Proper segregation of duties is required, especially among operating system engineering, application System design, and data control.

- Employee security policy
  The employees should recognise and comply with security policies.

- Information assets management policy
  Important information assets should be managed by specified employees; risks and protection measures should be assessed periodically.

- Software policy
  The implementation of software should be conducted by a team which consists of members from IT, accounting, auditing and the end user. Risks should be assessed in advance, and all security measures should be made ready before on production.

- Change policy
  Any change in computing environment should be conducted under approval. Detailed evidences should be kept and reviewed regularly.

- Data access security policy
  Each application system should properly take into account the various access requirements to define various access rights.

- Disaster Recovery Plan & Business Continuity Plan
  DRP & BCP should be properly planned for each application system, and periodically exercised.

- Physical and environmental security policy
  Information security requirements should be considered in office areas and restricted areas, and enforced practically.

- Network security policy
  Secure data transmission in internal and external networks should be also properly planned and enforced.

- Outsourcing policy
  In case of outsourcing, risks should be assessed in advance. Proper risk mitigation measures should be planned in advance and enforced.

- Legal compliance policy
  Laws, regulations and any contracts that are applicable to IT-related activities should be periodically reviewed for compliance.

- Internal auditing policy
  Periodic internal auditing should be conducted to ensure the soundness and compliance in IT-related operations.

References

Electronic Banking Group of the Basel Committee on Banking Supervision, BIS, "Risk Management Principles for Electronic Banking", July 2003.

Electronic Banking Group of the Basel Committee on Banking Supervision, BIS, "Management and Supervision of Cross-Border Electronic Banking Activities", July 2003.

Michale Juergens, Deloitte & Touche LLP, "Management of IT Auditing", Global Technology Audit Guide, The Institute of Internal Auditors, March 2006.

Michele Braun, James McAndrews, William Roberds and Richard Sullivan, "Understanding Risk Management in Emerging Retail Payments" *FRBNY Economic Policy Review*, September 2008, Volume 14, Number 2.

Tzong-Chen Wu and Shi-Cho Cha, "On the Design of Security Mechanisms for e-Payment Systems", *Taiwan Banking and Finance Quarterly*, Vol. 8, Number 2.
Financial Statistics Monthly, Republic of China (Taiwan)

<http://www.cbc.gov.tw/economic/EBOOK/WWW/cbc_menu_en.asp>
Condition and Performance of Domestic Banks, Republic of China (Taiwan)

<http://www.cbc.gov.tw/EngHome/Ebankexam/Statistics/eubpr/Current/index.asp>, Payment Systems, Republic of China (Taiwan)

<http://www.cbc.gov.tw/EngHome/payment.asp>

CHAPTER 10

THE SUPERVISORY IMPACT OF TECHNOLOGY ON SEACEN FINANCIAL INSTITUTIONS: ISSUES AND CHALLENGES IN VIETNAM

by Phan Thai Dung[1]

1. Introduction

In the international economic integration process, the banking system is very important. A banking system which operates effectively is essential for the optimal allocation of financial resources which ultimately stimulate growth . However, in a market economy, risks in banking operations are unavoidable and can lead to adverse chain reactions. The collapse of a bank has negative impacts on the socio-political-economic situation in a country and could spread across borders.

The Vietnamese banking system, which has switched to a market based one, has developed in depth as well as breadth. Banks are the most important financial institutions in the economy. The commercial banks make up the biggest proportion in terms of assets, market share and numbers. Banks have gradually evolved and are using technology to provide the best services for the customers. However, in the process of innovation, Vietnamese banks' operations have faced serious risks from the application of information technology. This research study is undertaken to analyse issues and challenges of supervising operations of information technology and also explore steps that can be taken to overcome the challenges.

2. The Overview of Financial Institutions

The establishment in 1987 of the first commercial joint-stock bank in Vietnam- the Sai Gon industrial and commercial joint-stock bank, initiated the promulgation of commercial banks in Vietnam. The Vietnamese banking system has gained great strides. Currently in Vietnam, there are 5 state commercial banks, social policy banks, 37 commercial joint-stock banks (25 urban commercial joint-stock banks and 12 rural commercial joint-stock banks), 37 branches of foreign banks, 5 joint-venture banks, 45 representative office of foreign credit financial organisations, 5 financial companies, 9 financial renting companies, 904 people's credit funds and about 1635 branches. Among them, the commercial banking system plays a vital role in providing user-friendly banking services. However,

1 Author is Chief of Division of the Informatics Technology Department of State Bank ofVietnam.

in order to consider more objectively the progress as well as the limits of the commercial banking system in Vietnam, we need to consider the potential of banks in Vietnam.

First of all, the financial potential of Vietnamese commercial banks has improved considerably in recent times. However, the starting capital of the Vietnam commercial banking system is only about US$ 6.5 billion and total assets of US$ 60 billion.

Secondly, in term of profitability, the return on asset (ROA), and return on equity (ROE) of Vietnamese commercial banks are still low compared with the other countries in region. The ROE is about 9.99% to 44.88% while the ROA is about 0.7% to 2.91%.

Thirdly, in terms of the level of financial soundness, the bad debt ratio of all Vietnamese commercial banks has decreased sharply in recent years, from 8.5% in 2001 to 3,98% at the end of December 2007.

Fourthly, in terms of technological development, Vietnamese commercial banks have progressed rapidly to be on par with the more advanced countries in region. However, the technology application indexes of Vietnamese commercial banks are still far lower than many countries in region.

Fifthly, in terms of quality of human resources, commercial banks are still lagging in terms of appropriate training, professionalism and information technology know-how. The qualifications of banking staff are lower than other countries, especially in terms of executive and managerial skill and application of modern technology.

The commercial bank system was established during the first period of Vietnam's conversion process which is connected closely with the innovation process of the banking system. After nearly 20 years in operation, the commercial banks have undergone many challenges in their development. During the first period, the commercial joint-stock banking system met many with difficulties because the legal system was not sufficiently comprehensive and the regulations for banking operation have yet to be promulgated. However, with the implementation of the state's policy on commercial banks, the development of commercial banks has been rapid with some banks gaining huge strides in terms of branding and prestige in the domestic market.

From 2005 to now, the development of commercial banks have been stable. Their business activities are profitable with adequate provisioning for risk in accordance with regulations and the guarantee of a safety net in terms of deposit

insurance. Some commercial banks have a development strategy for the long-term from 5 years to 10 years which includes a clear orientation and direction on credit activities, foreign exchange, payment and new banking services (payment card, electronic banking, etc.)

For the improvement in services, the commercial joint-stock banks have attached special importance to modernising technology and broadening their activities through the new services such as factoring and Internet Banking. Some banks such as the Asian Commercial Joint-stock Bank and Technology Commercial Bank have been allowed to use risk preventive tools on the foreign exchange market such as dealing for account, interchange, option, etc. The commercial join-stock bank is better able compared with the state commercial bank for keeping up with international best practices. For example, recently the commercial joint-stock banks have put into practice, the government regulations on classifying debit and deduction using provision to assess credit risk more promptly and smoothly than the state commercial banks.

The rapid development of the commercial banks in the recent 5 years has proved their competitive ability. Brand names such as ACB (Asia commercial bank), Sacombank (Sai Gon Thuong Tin commercial joint-stock bank), EAB (East Asia commercial joint-stock bank), VIB (International commercial joint-stock bank), Habubank (Ha Noi Building joint-stock bank), Techcombank (Technological and commercial bank) are familiar with the population in the country through their credit products, financial services and support services.

However, the Vietnamese commercial banking system still has many weaknesses and lag behind somewhat compared with other banks in region and in the world. However, the banking system has made huge gains when compared to the first period (the period of innovation and conversion to a market economy). In the future, with the further development of our country, we believe that the commercial banking system will progress considerably.

3. Survey of the IT Implementation

3.1 Communication Conditions

In the "doimoi" period, Vietnam developed its communication infrastructure rapidly. From the beginning with only one state-owned company providing communication services, there are now five companies providing communication infrastructure, including two state-owned companies and three joint-stock ones. The competition amongst companies have increased the development of communication infrastructure. While the first company provided only landline services and X25 leased-line, companies are presently serving leased line cable with

broadband, applications and mobile phone services. The utlisation of services of the Vinasat satellite will make gigantic development steps for the communication infrastructure. In addition, some commercial banks have equipped the network with speed in the range of 1GB to 40GB.

In terms of the switch system, the International Gateway Switch is the most up-to-date switchboard generation in the world. The National Transit Switch is a modern switchboard which is capable of switching on the volume of information in the national network column. The Local Tadem Switches are located in Hanoi and Hochiminh City, with many other local switches located in provinces and cities. There are also satellite switchboards and subscribers' gathering systems. The Ministry of Post and Telecommunication of Vietnam (VNPT) has implemented a new generation of network NGN and is gradually converting the volume on PSTN into NGN as well as providing application services of NGN to customers.

Regarding the transmission network, the international transmission system consists of three international telecommunication centres with various switchboard systems, digital transmission linking the telecommunication network of Vietnam with the global telecommunication network. The international switchboards are connected to many different countries and transmitted through optical cables and satellites. Three centres of international telecommunication are connected to each other via an optical cable system capable of automatically processing problems and self-fixing. For trans-province transmission, the transmission network is on the North-South 20 Gbps optical cable backbone on the 1A national road and the 500KV electric line to ensure higher level of safety and wider band. This line also has another standby 140 Mbps satellite system, besides, other backbone lines of Viettel, etc.

The Transprovince transmission cable is almost opticalised while the transmission for the inner province is being extended and opticalised. The access network consists of three types – the local network, unwired subscriber system and VSAT system. The local cable network consists of copper cable and optical cable, providing telecommunication services to subscribers. The unwired subscriber system supports local cable networks and best suits high rise buildings and areas which are difficult to install the copper cable network. The VSAT system is used in mountainous areas and islands.

In terms of mobile network, there are already four providers selling services with two other providers preparing to sell national mobile services. MobiFone and Vinaphone of VNPT use GSM technology subscribed by 8 million users with capability to roam more than 84 countries. SPT uses CDMA1x technology, providing service from July 2003 and has currently approximately 0.14 million subscribers. From 2004, S_Fone, MobiFone and Vinaphone officially provided

messaging services across networks, accelerating the development of the mobile network. MobiFone and Vinaphone use GSM technology providing GPRS/ MMS preparation for the 3G strategy. Hanoi Telecom which uses CDMA2000 technology, is preparing to participate in the market. VP Telecom which uses CDMA450, is experimenting with its network and services in providing unwired fixed services. Local mobile networks consisting of unwired fixed phone and local mobile phone using IPAS system of PHS-IP technology are available in Hanoi and Hochiminh City.

In terms of Internet infrastructure, Vietnam has five providers providing internet services which are upgraded from dial-up technology to ADSL and high speed leased-line services. This development has created and improved the supply of Internet services of small companies directly to the public, leading to high volume of use of internet services from the public. As a result, credit institutions are also facilitated to provide Internet services to a relative high volume of clients. Young people make up a large proportion among the users.

International connection is implemented through six dimensions with the total band increasing from 1038 Mbps to 1892 Mbps. In terms of domestic connection, from 2003, IXP companies have implemented the same level of connectivity through VNNIC (Vietnam Internet Centre). Six companies are being licensed to provide Internet connecting services, namely VNPT, Viettel, FPT, SPT, ETC and Hanoi Telecom. Seven companies providing services to the public are VNPT, FPT, SPT, Netnam, Viettel, OCI and Hanoi Telecom.

According to VNNIC, as of year end 2007, total Internet subscribers reached more than 2 million with 0.5 million subscribers for provided IP. The wideband Internet access service has been available since 1997 including ISDN, leased line, VSAT. However, the client base is still small with the majority of users being institutions due to the high cost. From mid year of 2003, when VNPT provided ADSL services, up to now, there are three more providers of this service to the public namely FPT, Viettel and SPT. Currently, there are approximately 35,000 Internet access subscribers using wideband. Other types of Internet access services including Wifi and GPRS are also gaining popularity.

The number of Internet users is approximately 6.2 million; the density of Internet users is approximately 7.4%. Along with the number of subscribers and the number of Internet users, the number of Internet domain reflects the popularity of the Internet and the level of Internet application in socio-economic activities.

In terms of IT education, IT training modules have been included into the curriculum of primary schools. For ministries and industries, IT training has been included in the computerisation programme. On average, each official is equipped

with one computer. Specialised soft wares are also installed on the computers. 80% of activities are computerised. Companies which have Internet services are initiating online shopping. Laws on electronic transactions and online shopping have formed a legal framework for the development of e-commerce.

From 1980s, some universities have started to establish informatics faculties. Presently, almost all universities in Vietnam have informatics as a subject and students are trained in general informatics. Currently, there are about 15 universities providing basic training on informatics.

In 1990s, IT staff in Vietnam were employees who had switched from mathematics or physics disciplines. Currently, on the national level, it is anticipated out of 20 thousand employees, approximately 2 thousand people are specialised in informatics software. In addition, there are more than 50 thousand Vietnamese residing overseas working in this field.

Seven major universities in Hanoi and Hochiminh city and some mountainous areas are sponsored by the State to invest in faculties of information technology with the aim to generate 2 thousand IT graduates and software engineers each year. On average, approximately 3,500 people are being trained in basic informatics each year.

Apart from the faculties of informatics in universities, a number of information technology training centres have been established, contributing to the training of thousands of users and information technology officials.

12.3% of investment for information technology training reflects the current development of human resources applying information technology in banks. However, since this is an average rate, the allocation rate of training expenses of the different banks can vary greatly. However, in general, this reflects the banks' attitude for IT development. While banks are beginning to realise the importance of human resources in information technology, training however, has not been professional nor disciplined. More than 40% of banks surveyed responded that the only form of training on IT skill for employees is on-the-spot training, where employees are self-learnt and self-guided. Only a small percentage of banks are able to systematically coordinate different forms of training such as internal training courses, sending employees to attend training courses and on the job training.

Information technology qualification of employees in banks is currently rather low. (the rate of employees who can use computers average at 51%. The usage of the computer is limited to supporting specialised activities such as finance and accounting, internal management, etc). The level of awareness and

implementation of IT training as aforementioned, cannot meet the demand of the increasing application of information technology in banks. The survey results show that a close correlation between the rate of employees using computers and the training activities of banks.

3.2 Payment System

3.2.1 Interbank Payment System (IPS)

The Interbank payment system was established in February 2002. It operated simultaneously with the automatic clearing system. The transactions amongst the members of the system may be completed within 8 seconds. However, this system has not been set up in the whole country and is currently only operating in five big cities (Hanoi, Haiphong, Hochiminh City, Danang and Cantho). This system consists of two sub-systems: high value transfer system (HVTS) for transactions with a value over VND 500,000 (approx. US$ 33) and low value transfer system (LVTS) for the rest of the transactions. The design of the system was based on the Korean Interbank Payment System (KIPS), and was developed by Hyundai Information Technology Corporation. It is based on high-technology such as leased line, UNIX servers, and online database of banks. Recently, 81 banks participated in the system, with a total of 378 branches of commercial banks, credit institutions and financial firms. In 2008, the World Bank invested in the State Bank of Vietnam to develop and expand the payment system to the rest of the country.

If the balances at the State Bank of Vietnam (SBV) are sufficient, the transactions will be immediately transferred by the HVTS. Otherwise, the transactions will only be completed when there is sufficient balance in the account. The low value transactions are transferred to the LVTS, and at the end of the day they will paid by SBV through the clearing accounts.

Provincial payment centres (PPC) undertake local payments in the provincial areas. The inter-province transactions are transferred by bank members to the National Clearing System, and finally transferred to the receiving (beneficiary) banks.

3.2.2 Electronic Clearing System

This system, which was set up in 2002, was designed to replace the paper based clearing system. It is similar to the semi-automatic clearing system with each SBV provincial branch playing the core role in inter-province transactions. There are 58 provinces undertaking clearing in Vietnam. However, the clearing system will be replaced upon the implementation of the electronic payment system.

3.2.3 Credit Card and Debit Card System

Credit cards have been issued since 1996 by some domestic commercial banks. Up to April 2007, there are approximately 20,000 places accepting these cards at restaurants, hotels and supermarkets. In recent years, there has been a dramatic increase in debit cards in domestic banks due to their convenience for payment. Although appearing after credit cards, debit cards are more popular than credit cards, making up 95% in the number of cards.

Current credit cards used include Visa, Master and Amex. Currently, shops accepting credit cards still charge customers a fee of 3% of the total amount and remains a hindrance to users.

While some banks have issued credit cards for use in the domestic market, they are unpopular with the major places accepting these cards being shops or supermarkets collaborating with the banks.

3.2.4 ATM Card System

Currently, almost all banks have ATM cards with ATM withdrawal spots and ATM transaction POS. However, the ATM system has not developed sufficiently yet and is operating mostly based on magnetic technology. Currently, there are approximately 8.3 million domestic key cards and international key cards with the average annual growth rate of more than 100% compared to the previous years. There are 3 inter-institution cards - Smartlink, VNBC and Banknet. Since the beginning of 2008, Vietnam has linked all the ATMs of banks via the national financial switch company (Banknet).

While the ATM network has developed and expanded in recent years, it is still not widely shared yet, limiting the participation of users.

3.4 Online Banking Transaction

In Vietnam today, some banks are beginning to implement online banking services, enabling customers to use the Internet to conduct periodic transactions such as account balance checks, fund transfers within the same bank system, or payment of utility bills (electricity, water and phone). The following banks offer Interbank banking services:

- Vietnam Bank for Foreign Trade (Home banking and Internet banking)
- Vietnam Bank for Industry and Commerce
- Vietnam Technological and Commercial Joint- stock Bank (home banking)
- Asia Commercial Joint-Stock Bank (home banking and internet banking)

However, up to now, the scope of application for these services is still limited. Most banks have just begun to provide this service to a small base of customers such as major partners, credit institutions and companies. Transferring of money through the Internet is only conducted if the receiver's account is in a banking system. Although transfers and bill payments can be implemented online, the payment documents still require actual signatures, rendering the paying procedure an incomplete electronic procedure.

3.5 Internet Banking

In recent years, Internet banking in Vietnam has developed very rapidly. Some banks have introduced internet banking such as account access, online bill payments and transfers.

The regulation for vouchers have yet to be adjusted and payment orders that are transferred via the electronic medium (without actual signature of the account holders) do not have legality and are not accepted by banks. As a result, cards issued by Vietnamese banks cannot be used for online payments. This is a maor obstacle for transactions for online shopping. Internment is when all interactions between the sellers and the buyers are conducted online using electronic documents. In the effort to facilitate the payment medium for the customers, some goods/services suppliers are overcoming this obstacle with solutions depending on the situation.

3.6 Mobi Banking

Although the Mobi Phone is very popular with more than 10 million users, Mobi Banking is still at the initial stages of development. Considering the potential of Mobi banking, some banks have provided their customers with services such as phone payment, internet payment, balance checking and transfer through accounts.

3.7 Electronic Cash and Prepaid Cards

Presently, electronic cash is in the form of card usage such as phone cards, internet cards, prepaid mobiphone cards which are very common for telecommunication.

In recent years, the bank system of Vietnam has developed rapidly in terms of the quantity of banks. Banks have invested in modern information technology to better meet the demands of customers. However, the implementation of information technology depends on the abilities of people, finance and the development vision of each bank.

State-owned commercial banks which have been in existence for a long time have made huge investments in modern technology. However, there are still many newly established banks which face difficulties in areas such as capital, technology and skilled people. As a result, information technology has not been sufficiently invested in by these new banks to meet the challenges in competition and integration.

While some banks have chosen to outsource for solutions from overseas, some banks have opted to hire domestic companies to develop solutions, with some banks even taking upon themselves to develop their own internal solutions. Therefore, the differences in the levels of technology of banks and the use of different technology have affected the application of technological standards and the supervision of information technology.

Are the following IT Infrastructure installed in the Vietnam?

No.	Item	Yes/No
1	Communication Network	Yes
	Cable (Phone line)	Yes
	Satellite	Yes
	Fiber Optic	Yes
2	Use of Cellular Phone	Yes
	Is it relatively wide spread?	Yes
3	Use of Internet	Yes
	Is it relatively wide spread?	Yes
4	National Payment System	Yes
5	Operated by government agency / central bank	Yes
6	Operated by an independent or private company	No
7	Automated/Computerized Payment System	Yes
8	RTGS	No
9	National Securities Settlement System	Yes
	Operated by government agency / central bank	Yes
	Automated/Computerized Settlement System	Yes

Are the following IT Infrastructure installed in the Vietnam?

No.	Item	Yes/No
1	Communication Network	Yes
	Cable (Phone line)	Yes
	Satellite	Yes
	Fiber Optic	Yes
2	Use of Cellular Phone	Yes
	Is it relatively wide spread?	Yes
3	Use of Internet	Yes
	Is it relatively wide spread?	Yes
4	National Payment System	Yes
5	Operated by government agency / central bank	Yes
6	Operated by an independent or private company	No
7	Automated/Computerized Payment System	Yes
8	RTGS	Yes
9	National Securities Settlement System	Yes
	Operated by government agency / central bank	Yes
	Automated/Computerized Settlement System	Yes

Are the following IT-related products implemented in Vietnam?

No.	Item	Yes/No
1	Credit Card	Yes
	National (only used in the country)	Yes
	International	Yes
2	Debit Card	Yes
	National (only used in the country)	Yes
	International	Yes
3	ATM	Yes
	Individual bank	Yes
	Nationally-Shared ATM	Yes
	Internationally-Shared ATM	No

4	Electronic Fund Transfer (EFT)	Yes
5	EFT at Point of Sale	Yes
	National (only within the country)	Yes
	International	Yes
6	Remittance Service	Yes
	Domestic companies	Yes
	International companies	No
7	Phone Banking	Yes
	Informational	Yes
	Transactional intra bank	Yes
	Transactional inter bank	No
8	Mobile/SMS Banking	Yes
	Informational	Yes
	Transactional intra bank	Yes
	Transactional inter bank	No
9	Internet Banking	Yes
	Informational	Yes
	Transactional intra bank	Yes
	Transactional inter bank	No
10	Pre-paid card	Yes

Regarding IT-related Applications in addition to IT-related products, are the following applications implemented with IT?

No.	Item	Yes/No
1	Core Banking: General Ledger, Third Party Fund, Loan, and Consumer Information File	Yes
2	Treasury	No
3	Remittance	Yes
4	Trade Finance	No
5	Corporate Online Service	No

4. Impacts of IT Implementation on Financial Institutions

4.1 Operational Risks

To effectively manage the operational risks arising from the operations of information technology system, banks have to assess the specific and general operational risks. General operational risks include:

- Technical risks: Risks arising from the technical system
- Human risks: Risk arising from technical staff
- Risks arising from people using the products and services
- Risks from the third-partyimplementing warranty and maintenance
- Risks caused by lack of operational processor incorrect operational process
- Risks caused by the impact of environment.
- Risks caused by attacks

4.2 Technical Risks

Technical risks always arise from the errors of information technology. In order to have a good information technology product, there must be compliance in the deploying process via the following steps: general design, design detail, selection of technology, software design, proper testing, testing in the actual environment and implementation. If we these processes are not well supervised, the product may not meet requirements. In the process of deploying products, information technology will face risks of unusability and have this have major implications on cost and wasted effort.

4.3 Human Resource Risks

Human resources are important factors in the implementation of financial products. The selection of the system-designer is a very important process. A well designed product will help avoid many risks in the financial product. To minimise risks, in the process of selecting the provider, the institutions must rigorously test the aptitude of staff deploying the financial products. With a good deployment, the hand over to the technical staff will be much smoother and efficient.

4.4 Risks Arising from People Using Financial Products

New products will have risks from users if the products are not user friendly. If the interface and structure are too complicated, users will be confused. Training and guidance for the users are important elements in the process of introducing the applied products to users.

4.5 Risk from Third-Party, Warranty, Maintenance

In cases of external leasing and collaborations with third-parties that provide financial products, the financial institutions must carry out the following steps. Firstly, they must assess the specific risks, supervise and ensure information security. Secondly, they must have backup solutions in case third-parties are not available. Thirdly, they must appraise the technical and the financial capabilities of the third-party. Fourthly, the clauses of agreement with the third-party and assignments of particular responsibilities for each party muct be clear and lucid. There must be penalty clauses if risks occur. Fifthly, they must monitor and assess the coordination process of the third-party.

4.6 Risks Caused by Lack of Operational Process or Incorrect Operational Process

During the process of deploying technology, the trial and test scripts must be established in case of unforeseen circumstances and these must be built into the operational process. The operational process will continually be perfected in the trial periods in the actual environment. Establishing a good operational process has very significant influences on the success of applying financial services.

4.7 Risks Caused by Impact of Environment

The environment, such as power source, air-conditioning, exit and entrance, windows, alarm-system and etc., has an impact for the application and deployment of information technology. To avoid risks of systems failure, attention has to be given on building the right physical environment, the processes, the regulations, the technical standards, the technical parameter to ensure security.

4.8 Risks Caused by Attacks

Hackers are increasingly wrecking more havoc on the IT systems of the financial institutions with more sophisticated technology causing major damages. To avoid such occurrences, these risks have to be assessed at the outset from the very inception of the system. Security solutions capable of preventing such risks must be in place commiserating with the level of services and expenditure of the financial institutions.

Vietnam is in the process of integrating and developing its financial system and many credit institutions are competing in order to provide the best IT-applied services for customers. Coming out with IT services that are not sufficiently secure will have many risks.

The choice of suitable technology is a very difficult task. As the general standards have not been established, the choice of technology in financial institutions is currently very much dependent on the technological provider or by gut feeling. As a result, some institutions choose unsuitable technology leading to project failure and wastage of resources. To overcome this, the general standards for all financial institutions should be established to prevent risks.

Vietnam has developed the system for training in information technology. There many universities majoring in training human resources for information technology such as FPT University, Encyclopedic University, and Natural Scientific University. Moreover, every university has its own informatics technological faculty. However, universities are just providing the basic knowledge because they lack the physical facilities for in-depth training. After university, the institutions have to retrain the graduates for specific requirements. Many financial institutions usually require IT personnel to have professional experiences. The qualifications of IT personnel have significant influences on the training time. Currently, some IT companies as well financial institutions have established their own training schools to solve their personnel issues.

80% of Vietnam's working population are involved in the agricultural sector. Financial institutions therefore face many difficulties in introducing financial products for the people due to their lack of knowledge and perceptions. The economy is still very much a cash based one. In recent times however, the government has initiated a policy of " using less cash", which encourages the credit institutions to introduce products which uses less or no cash in the market. However, in response, the financial institutions have just provided mainly ATM services. The major customers are usually the state staff, big companies and enterprises that have the salary payments through accounts.

The electronic commerce of Vietnam is still under developed and has just mainly stopped at providing WEB and basic products. There has not been cooperation between the financial institutions and the services seller yet. The government has initiated the law on electronic transactions, establishing the legal foundation for enterprises providing electronic commerce.

Some financial institutions have not attached special importance to investing on IT environment. Many do not have internal power sources in case of power cuts, proper fire prevention system, efficient air-conditioning for IT hardware, and systems for controlling entrance and exit. These systems require high initial outlays in terms of finances. As there are insufficient investments for the supporting environment, the associated risks for customers are also high.

In recent years, the financial institutions have paid special attention to ensuring security and prevention of unauthorised incursion into their IT systems. However, risks of hacking remain due to the lack in investments for properly trained human resources. However, since Internet financial products and services of the financial institutions are still not very significant, the risks are not excessive.

IT Risks

On the impact of the level of IT Implementation in the country, what are the risks that need to be addressed and controlled in the financial system?

No.	Item	Yes/No
1	Operation Risk	Yes
2	Liquidity Risk	Yes
3	Credit Risk	Yes
4	Strategic Risk	Yes
5	Reputation Risk	No
6	Legal Risk	No
7	Compliance Risk	No

4.9 Strengths and Weaknesses of Supervisory Procedure in Vietnam

Currently, some long established state financial institutions have implemented the necessary regulatory framework for controlling risks. However, some of the smaller financial institutions which do not have an extensive IT system have not placed not much emphasis on establishing a regulatory framework for IT. IT supervision in Vietnam is carried out by an internal IT audit division. The financial institutions which have regulatory frameworks such as security policies would have risk prevention policies. In this regard, the internal audit division will have overall charge of policies, regulations and processes. In case of policy infringements by the audit division, the supervisor will have the overriding authority to make rectifications.

Information technology of financial institutions is still at the initial state of development in Vietnam. Investment in new facilities and advanced technologies would reduce risks from obsolete technology. Financial institutions of Vietnam have many opportunities to learn from experiences of foreign financial institutions on the application of information technology and training of personnel.

However, IT supervision has not gained much ground as administrative procedures and processes have yet to be properly established and tested to assess risks. In addition, there have been little emphasis on financial institutions' risk due to the following reasons:

- The qualifications of supervisors have yet to meet necessary requirements and training is still insufficient. Many do not have experience in IT.

- The framework and procedures are insufficient and there is no clear responsibilities of IT staff in providing information to supervisors.

4.10 The Main Directions

- Better training for the supervisors.

- Perfect the regulatory framework and responsibilities in providing information for supervisors.

- Equip the system with advanced information technology, ensure security, reduce risks, and apply digital signatures and the technology confirming users such as biometrics, fingerprint scans, etc.

5. Prevailing IT Supervisory Framework and Regulations

5.1 Present Supervisory Framework and Regulations

IT services in Vietnam are very diversified with no general standards for financial institutions. Investment in technology of each financial institution depends on their requirements and limits in expenditure. Some financial institutions acquire their IT solutions from foreign countries for local application while some medium and small-scale companies opt to hire domestic companies to develop solutions. Some small scale services are developed by internal IT staff of the financial institutions. With this diversification, assessing and controlling risks are very difficult. Financial institutions should take their own responsibility on IT risks. In Vietnam, there is no regulation of IT supervision for the financial institutions. There is currently only one document on information security for credit institutions. The implementation of security features has yet to be emphasised due to the following reasons:

- Vietnam has about 100 financial institutions which are very diversfied. Controlling risks in IT would require a large IT workforce.

- The regulatory framework, procedures, standards for control risks have not been widely established. There are also no sanctions to deal with violations.

To implement supervision and assessment of IT risks in the financial institutions, there is need to:

- Develop IT supervisory staff who have the ability and technological qualification to manage IT.

- Develop a regulatory framework, procedures and standards to manage IT and use professional tools to assess risks.

5.2 Building a Supervisory Framework to Control IT Risks

- Unify managing and controlling risks of information technology in banks' operations

- Actively prevent and restrict IT risks in bank's operations

- Define responsibility, authority for every individual, organisation in managing and controlling risks in banks'operations.

5.3 Discuss the Regulations in IT Supervision

This includes regulations and guiding operations to audit IT. In order to supervise IT, we need to have the specific regulations according to the product's cycle. This process should be in place at the planning stage before the products are applied on a big-scale:

- Plan and project: The development strategy must a general one. We must define the development incentive, the market needs for products and services (includes the economic-socio-technological factors)

- Define the development potential of market through estimating market needs, assessing competitive competence in comparison with competitor in providing products and services of banks.

- Consider administrative ability and control risks. Compare between the risk administrative ability and the level of applying of the financial products and services

- Building projects: Define the general target and the quantitative target specifically for each financial product and service.

- Define risks: We must consider the risks and propose forward solutions to deal with main potential risks of financial services which may consist

of the following: demonstrative risk, prestigious risk, legal risk, risks involving customers and third-party. The potential risks must be mitigated arising from the implementation of the financial products and services. Hence, it is necessary to define the degree of maximum damage that the financial institutions have to suffer in the provision of financial products and services and there must be solutions for management for each form of risk.

5.4 Build Specific Deployment Plan

This includes finance, deploying itinerary, technological risk, facilities, personnel and other involved problems.

- Assign a duty to each member; build a plan to provide financial products and services. There is also a need to specify responsibility for each professional division, technological division, and administrative division.

+ Responsibility of professional division: take responsibility for building procedures; stipulate the professional competence for the financial products and services.

+ Responsibility of technological division: Establish an application programme, ensure safety and security, effectiveness, and compliance with the legal regulations and international integration; frequently check, assess and propose forward solutions for processing risks for each specific application.

+ Responsibility of administrative division: Divide the responsibilities among the members clearly to meet requirements of operations thoroughly; carry out and supervise the technical process, other organisational management; operate and supervise software, hardware, communication network, database, information system.

+ Responsibility of division for checking, collecting and analysing risks in financial products and services. This division makes periodic and unannounced inspections, checks the system of the financial products and services to minimise risks in financial products and services. The risk management division takes responsibility for collecting, analysing and reporting any breakdowns in financial products and services.

+ Responsibility for the third-party which must adhere to the following steps:

Assess all risks completely and the effect of each risk on operations, reputation, brand name of the bank; assess solutions on information security based on the overall solutions of financial institutions and third-parties. There should be spare solutions in case of interruptions or unavailability of third-party solutions. The technical ability and the financial capacity of the third-party must be assessed properly. In the contract with the third-party, the responsibilities and authority of each party must be defined as well as the usage of logos in the process of providing the financial products and services. The financial institutions have the right to make periodic checks on the provision of technical-support services of the third-party as well as the collaboration and cooperation process such as potential risks, level of safeness, data security in the present and in the future and suggest solutions to enhance the systematic security and data security.

5.5 IT-specialised Supervisor/Auditor

In Vietnam, some of the state commercial joint-stock banks sometimes transfer staff from the IT division to IT audit division and some from the professional divisions to IT divisions. Some professional auditors double up as IT auditors.

Training for IT supervisors is still insufficient. The IT division takes the main responsibility for deploying IT and training is usually only in the form of technological transfer. Therefore, IT supervisors are not properly trained nor supervised to identify risks in the new system. Supervisors are expected to take over after the IT process has been put introduced and they therefore do not have the ability to detect the errors in the process. To increase the level of expertise for IT supervisors and auditors, there should be specific training programme for IT staff.

Basic knowledge for IT staff must cover every aspect from hardware, software to information security, etc. IT staff must have the basic knowledge at least to understand the operational regulations and detect weaknesses of system.

In the process of deployment and transfer of information technology training, it is very necessary to encourage the supervisor's participation in order for him/her to gain the basic concepts of the project, facilities, software and technology used.

For institutions (e.g., financial companies within the postal corporation, petrol corporations) that that do not fall under the IT risk management of banks, the control of their IT risks is undertaken by their management offices. In Vietnam, overall IT management is the responsibility of the department of information and propaganda of the government. The department of information and propaganda

will initiate regulations such as law on information technology, law on electronic transaction and digital signature. The units have to comply with the regulations of the government and the department of information and propaganda. However, there is yet to be any legal framework to manage risks of non-bank institutions. Currently, the use of technology in non-banks financial institutions is based on the agreement between the non-banks and their customers. However, as IT applications in non-banks are still minimal due to the lack in professional competency, the associated IT risk remain low.

Regarding IT supervisory framework

No.	Item	Yes/No
1	Is IT Implementation reported regularly?	Yes
2	Is IT audit conducted?	Yes
	By bank/IT supervisors from supervisory authority	
	Off-site	Yes
	On-site	
	By internal or external (third party) auditors (on-site)	No
	Special IT audit/examination outside regular examination (on-site)	No
3	Does the formal framework exist?	No
4	If yes, is it stipulated in a regulation?	No
5	Is there minimum requirement in IT Implementation? Are the following items implemented:	
	Active supervision by Top Management (IT Steering Committee)	No
	IT Policy and Standard Operating Procedure	No
	IT risk is included in the risk-based management	No
	System development life cycle	Yes
	All layers of IT system	Yes
	Internal control system for IT Implementation	No
	Business Continuity Plan and Disaster Recovery Plan	Yes

	Periodical IT audit (internal/external)	No
5	Because it involves supervision procedure, is IT outsourcing especially regulated?	Yes
6	Because it involves consumer protection, is E-banking products especially regulated?	Yes
7	Are any IT-related laws (cyber law, e-commerce, m-commerce, digital signature) installed?	Yes

Regarding on-site IT Audit,

No.	Item	Yes/No
1	Is it conducted regularly?	No
2	If not regularly, is it conducted case by case?	Yes
3	If regularly, objects of audit:	No
	Organization and Management	
	System development process	
	Operation	
	Software and Application, including E-Banking	
	Security (authentication, authorization and protection – including audit trails, encryption)	
	BCP/DRP	
	Communication Network	
	Outsourcing process	
	Internal Auditing	

6. Issues and Challenges

6.1 Issues

Vietnam is in the process of integration and development and IT application is, therefore, still rather new. In order to develop IT and prevent risks, we need to establish policies for change, update the knowledge of new IT application for staff at management levels. It is only from there that we can implement IT strategies and legal frameworks.

In terms of human resource potential, as Vietnam is still developing, the need for IT personnel is very urgent. There is still a lack of institutions of higher learning emphasising on IT. To rectify this, some universities have initiated more disciplines concentrating on information technology. However, it is also realized that the qualifications of IT graduates are not able to meet the requirements in the work environment and it normally takes about 1 to 2 years to retrain IT personnel.

In terms of reimbursement, salaries of IT staff in financial institutions are far lower than the major corporations and the IT specialised companies while salaries of IT staff in state banks are even lower than other financial institutions and securities companies. In recent years therefore, there have been many turnovers in IT personnel of financial institutions, causing an imbalance in IT staffing among institutions. Security companies have attracted many IT staff who have worked for the financial institutions, causing a shortage of IT personnel in financial institutions.

Since information technology in Vietnam is still very new, financial institution are at the initial stages of IT applications. These institutions are in process of initiating the legal framework and the regulations to supervise information technology innovations and avert risks.

Transfer of technology between countries is still limited for Vietnam as it has just recently joined the WTO and other regional organisations. Moreover, professional ethics are still a shortcoming in financial institutions. There have been incidences where staff having IT savvy, have siphoned funds from financial institutions and customers as supervision is still weak.

6.2 Challenges

Vietnam is in the innovation process and its IT infrastructure is still backward, yet to meet international requirements. However, communication and the internet-lines with high speed are being developed and built in 63 of provinces and cities.

The equipment and facilities in the credit institutions are still insufficient due to financial limitations. Human resources in IT is still lacking in terms of qualification and quantity and there is a general lack of experience in implementing financial IT.

The top management level of financial institutions has not taken the operation, deployment and implementation of IT seriously. In addition, hackers have, in recent years, attacked and violated the IT systems of some financial institutions due to weak security systems and facilities.

7. Policy Recommendation

IT risk can pose great losses both in terms of costs and reputation of financial institutions. In order to reduce IT risks, there is a need to increase the awareness of the top management. The IT units must make regular updates and reports on risks to management for arriving at solutions and forecasting future potential risks.

7.1 IT Risks Policy

Before initiating policies, the following main risks must first be defined - demonstrative risk, reputational risk, legal risk, customer risk and the third-party risk. The estimated risks and the maximum damage from risks that the institutions can suffer from have to be defined.

The ability of administering and controlling risks and the ability of the internal controlling system in supervising risks to ensure operations security in IT systems must be in place. In addition, there is also the need to define the specific time -points in carrying out the proposed target, establish the plan of checking and assessing the implementation state of the project's content.

The responsibility among units must be equitably allocated, namely units responsible for IT implementation in the professional division, technological division, systems management division as well as users' responsibility.

7.2 The Supervisory Framework

The supervisory process must be improved systematically in order to ensure the proper assessment of operations in financial products. Inspection and supervision must ensure that confidential information involving customers at financial institutions are secure. There should be provisions against the usage of information for purposes contrary to regulations and they should not also be revealed to third-parties.

7.3 FI Supervisor and IT Auditor

FI supervisors and ITs auditor must comply with regulations and professional procedures to ensure compliance and the safe and secure application of IT products. They must inspect IT systems periodically or randomly to minimise risks in IT system.

The IT system programme must have functions of reporting, inspecting and management including:

- Journal on system cable
- Transaction journal
- System value journal
- Other reports

The internal inspection and supervision for IT must have the proper procedures and guidelines for internal inspection and supervision. According to the level of risk, the internal inspection and supervision for IT operation should include the following contents:

- Inspecting access action
- Inspecting copyright
- Inspecting current data and stored data
- Inspecting compliance of procedures
- Inspecting current file in usage

8. Conclusion

Currently, Vietnam is a developing country with a low per capita income. Hence, this is one main reason for the limited development in IT applications of financial institutions. Other factors include are lack of funds/resources to invest in IT modernisation; lack in technology know-how and training.

Closing the financial IT gap between Vietnam with other countries and the rest of world would require the government giving focus on investments with sizeable capital for IT (such as hardware, software, network and telecommunication education, innovations in products, software, automation in banking services, etc.). Establishing a technical base for an open cashless payment services and developing new services for financial institutions should be given preference in the development of financial IT. The next step would be to upgrade and improve the national payment system. To minimise risks for financial institutions, the supervision of IT products and services should be prioritised.