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

by G.K.K. Gamage¹

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)	23
Domestic Banks	11
Foreign Banks	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

<u>No.</u>	<u>Item</u>	<u>Yes/No</u>
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.

<u>No.</u>	<u>Item</u>	<u>Yes/No</u>
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

<u>No.</u>	<u>Item</u>	<u>Yes/No</u>
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 of 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

<u>No.</u>	<u>Item</u>	<u>Yes/No</u>
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

<u>No.</u>	<u>Item</u>	<u>Yes/No</u>
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 possesses 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.