Chapter 7

IT Security, Audit & Controls in Banks:
Issues and Suggestions
Chapter 7

IT Security, Audit & Controls in Banks:
Issues and Suggestions

7.1 Introduction
In Chapter 6 dealt with the recent developments in the field of IT-based banking both in developed
countries as well as in India. Some of the products of E-commerce, Internet banking, E-cards, EDI,
EFT are not yet fully free from unauthorised accesses, attacks and therefore frauds. In this chapter,
therefore, issues are identified in this regard, and remedies to overcome them related to IT security,
audits and controls with particular reference to Indian banks, are discussed.

7.2 Information Security
Most of bank related information is created by or directly linked to computer processing. This
includes customer records, financial transactions, business strategies, software systems, and even
corporate correspondence. Financial data and business documents routinely are transmitted
throughout a bank corporation through floppies or via telecommunication lines linked to computers.
Similar information also is transmitted outside the corporation, between the bank and its
 correspondents, its regulators, and its customers.

Information, regardless of its source, is a valuable asset to the bank. Its accuracy and confidentiality
are essential to the business. Accordingly, it must be protected from abuses such as inadvertent or
intentional misuse, disclosure, fraud, and error. Information systems, both the data and the software
that creates and stores the data, must be secure.

Data are created and stored in substantial volume, often representing millions of bank records and
transactions. Correspondence and bank strategies also are created and stored through text processing.
Bank customers’ funds are routinely transferred via computerized payment networks. Transmission
of these data regularly occur over public communications links, such as telephone lines and satellites.
In addition, many users, including employees and bank customers, can directly access the data
through computer terminals or telephones. Some have the ability to change information or create new
data. These activities, while improving customer services and internal operations, also have increased
the risk for error and abuse of the bank’s information.

Controls must exist to minimize the vulnerability of all information and to provide necessary security.
The level of control must be assessed against the degree of exposure and the impact of loss to the
institution. This includes financial loss, competitive disadvantage, damaged reputation, improper disclosure, lawsuit, or regulatory sanctions.

Various processes are available to strengthen information security in the banks. The most basic are sound written management policies for internal controls. These include physical security, separation of duties, quality control, hardware and software access controls, and audit.

Information security controls should be designed to ensure the integrity and accuracy of management information systems, prevent unauthorized alteration during data creation, transfer, and storage, maintain confidentiality, restrict physical access, authenticate user access, verify accuracy of processing during input and output, maintain backup and recovery capability, provide environmental protection against information damage or destruction.

Computer hardware and software technologies can help protect information resources. Although they vary, security features usually are available at each level of computer sophistication. Regardless of the controls adopted, they should apply to information produced and stored by both automated and manual methods. Suggestions on areas of risk and technology controls are given below.

Information security is a functional responsibility. And as a means to protect assets, it must be a strategic objective of the business. A sound system of internal controls and management policies must be established and enforced to satisfy this objective. The Board of Directors should require that information security policies exist throughout the bank/corporation. These policies must be in writing and communicated to all personnel and other authorized users of bank information systems. IT Auditors may periodically target reviews of information security in the bank’s supervisory strategy. These reviews may include the adequacy of the “corporate information security policy”, compliance with the security standards, and management’s supervision of these activities.

Some risk exists in every system and operation of the bank, whether manual or automated. Management must recognize the types of systems and operations that pose greater risks to information security. These might include mainframe computer operations, microcomputer operations, communications networking, operating systems, applications software, end-user computing, distributed processing networks, system recovery activities, information retention and backup, text processing (office automation), document filing and retention, manual departmental operations.

Technology controls for information security must include (i) Encryption - a process by which plain text is converted into encrypted strings of meaningless symbols and characters. This helps prevent
unauthorized viewing and altering of electronic data transactions during transmission or storage. The Data Encryption Standard (DES) is commonly used for encoding PIN numbers on access cards, for storing user passwords, and for funds transfers on large value payment networks. (ii) **Message Authentication** - a code (MAC) designed to protect against unauthorized alteration of electronic data transactions during transmission or storage. This code is used with data encryption to further secure transmission of large dollar payments. (iii) **Security Software** - application software designed to restrict access to computer-based data, files, programs, utilities, and system commands. Some systems can control access by user, by transaction, and by terminal. Security violations, including attempts can be reported and access reports also can be produced, (iv) **Data Retention** - the internal operations that require critical bank records to be regularly copies and stored in an offsite location. This includes data files, programs, operating systems, and related documentation. This also applies to critical data produced in hardcopy documents.

These are a few examples of controls and technologies to assist information security. New technologies and security methods are being developed and introduced constantly. The type and extent of controls must be measured against the degree of risk in any activity.

### 7.3 Internal Controls

Data Security should be addressed prior to the installation of such a system. Existing data security systems may not be adequate for a complex integrated system, particularly when using on-line real-time processing. Each individual function should be controlled, e.g. access controls, file maintenance, inquiry, and new accounts.

IT-Auditing prevents chance of unwarranted data manipulation through diminished audit trail. Therefore, institutions should recognize the need for expanded IT-audits of this technology, especially in an on-line real-time environment.

While conducting such an IT-audit exercise, it is necessary to adopt a functional-approach. Therefore, the aspects which need to be looked into while conducting such IT-audits include: IT strategic planning, IT organisation, IT sites, data-processing operations, back-up operations, software systems, system access controls, PCs (Personal Computers), software maintenance, LANs (Local Area Networks), databases, IT-facilities management, system development, software selection, contingency planning, Electronic Data Interchange (EDI) and Electronic Funds Transfer (EFT) systems, viruses, office automation systems, etc. Based on the discussions with the IT-auditors, IT-heads/Chiefs of CPPD and other senior executives from IT departments of the banks in India, during various training programmes / workshops / conferences held at NIBM during 1995-1999, certain
control-issues and control-measures related to some of these aspects have been identified. The same are highlighted in Appendix 5.

When a system allows the automatic generation of a transaction prompted by a prior-transaction, controls must be designed within the system to ensure satisfactory audit-trails. This is especially critical considering that a single transaction may generate several other transactions.

Accountability for all transactions must be maintained through audit trails. Otherwise, system integrity deficiencies will jeopardize the software system’s ability to provide a consistent product, as well as compromise internal controls.

Existing generalized audit software may not be readily adaptable for use with large-scale integrated systems, and may not be sufficiently sophisticated to follow an audit trail of all transactions generated by the system. Therefore, there is a need to develop audit software depending on type of the applications in use consistent with different types of technological platforms on which these applications run. Some of these applications generate large amount of information for the use of managerial decision making and when integrated result into large scale integrated MIS.

7.4 Large-scale integrated MIS

Banks and FI’s have experienced problems in their attempt to introduce TBA (Total Branch Automation) and especially integrated Management Information Systems (IMIS).

Bank and FI executives should be aware of and concerned about the potential problems with integrated MIS. These institutions would be exposed to the risks associated with these systems and, therefore, it is necessary to identify management’s responsibilities when entering into an integrated MIS and DSS (Decision Support System) projects.

“An integrated software system is one in which programs for different applications—loans, deposits, retail, and wholesale—that normally are designed and operated as stand alone programs are built from the start as related parts of a whole. They share a compatible data, application SW systems, and other technical details so that they can be made to ‘talk’ to each other with relative ease. More importantly, they function as one unit so that the sum of the parts is greater than the whole”.

Financial institutions are adopting integrated MIS approach in order to meet competitive pressures, increase in timeliness of information, foster operational efficiency, and ease introduction of new products. A commitment to IMIS sets the course of an institution’s technology, management information system, and delivery systems for several years.
Successful implementation of IMIS requires careful planning by both senior management and the board of directors. Ineffective planning caused several banks, FIs and software companies to spend lakhs of rupees and lot of conversion and implementation time on IMIS, only to implement a portion of the system or in some cases abandon the project altogether. In many instances, the software vendors depended upon substantial ongoing investment by the banks to indirectly fund the vendor’s research and development process, rather than banks’ own development. When these projects experienced lengthy delays, the banks not only suffered large monetary losses but also delays in product development and a loss in their competitive position.

Many banks have underestimated the cost, time and personnel resources required for the successful installation of IMIS. Therefore, time and cost targets should be established at the beginning of the project and closely reviewed by senior management on an ongoing basis.

In certain cases, IMIS projects were abandoned because of the financial instability of software vendors. To prevent these situations from recurring technical competency, the financial condition and viability of each prospective vendor must be considered when evaluating systems.

Data backup and recovery measures for integrated systems are often more costly than those required for single application systems. In certain situations, the database may require on-line/simultaneous backup. The additional costs for backup and recovery must be evaluated when determining the feasibility of IMIS.

If the system provides for instantaneous update of information - in other words, the user has direct access to the data, existing security systems may not be adequate. Thus, data-security features must be evaluated to ensure that sufficient controls exist for IMIS.

Seemingly simple program-changes can have unpredictable results in a mixed-application system. Thus, system development life cycle methodologies, which identify the sequence of activities required in the systems development process and throughout the useful life of the software, may need to be modified.

There is an increased possibility of undesired data manipulation and at the same time, there can be lack of an audit-trail in an IMIS environment. Therefore, IT-audit coverage should be reviewed at the onset to determine whether specialized audit techniques are needed.

Large-scale integrated MIS are sophisticated software products which provide interconnections and facilitate the exchange of information between applications and functions. The integration
architecture may be horizontal, tying together applications, such as deposits, loans, and general ledger. Alternatively, the architecture may be vertical, tying together functions, such as the output of the transaction-processing systems at branches being linked to the controlling and HO departments. These systems are designed so that each application no longer exists individually but operates as part of a unified system. They often employ database management technology, which increases the complexity of the system. IMIS processing may employ combinations of batch and online methods, on selective basis. A variety of IMIS are being marketed and others are in various stages of development. Some of the issues and weaknesses identified above can be overcome by following strategies.

The decision to acquire or develop in-house large-scale integrated software should be preceded by a strong and independent management planning process. This should include a thorough examination of existing software performance. Also, a detailed analysis of the system’s capability to meet the bank’s strategic business plans is essential.

The complexity of the software and its impact on the entire organization require a commitment from the top management for the project to be successful. Responsibility for the conversion should be clearly identified and established at the senior management level.

Senior management should regularly review the project’s status. This improves control over the complex process of implementation and ensures completion within established time and cost targets. It is particularly important that the board continues its oversight responsibilities after implementation.

Provision for audit software should be made at the time of system acquisition. Also Disaster Recovery Planning should be in place which will require a thorough consideration of contingency requirements in the initial feasibility study. The complexity of the integration, horizontally, vertically, or both, may not necessarily be determined by those current industry standards for the backup of hardware, software, data and communications. A determination should be made how the institution, as a whole, will recover and how recovery will be addressed along functional lines. Subsequently, the required testing may pose cost, logistical or other problems which will have to be resolved to ensure a viable disaster recovery plan.

Necessary changes in System Development Life Cycle (SDLC) Methodology should be ensured. There are several significant control issues regarding the use of traditional SDLC methods with large-scale integrated systems. Current system development techniques may not permit the timely development and implementation of a complex system. SDLC techniques may need to be revamped.
to provide for increased flexibility. However, control and management methods may vary according to the complexity of the system under development.

Management should carefully consider the cost of the extensive user involvement in the system development stage. User involvement is necessary to ensure the successful implementation of a large scale integrated system. Management must provide more comprehensive employee training since the adoption of an IMIS will affect all departments. SDLC standards need to be flexible, while still providing for the maintenance of system integrity during development to ensure that a system of internal control is maintained.

7.5 End User Computing Risks

In the recent years, microcomputers, or "personal computers", have become more prominent in the business environment. They are now being used, not only as word processors and access devices to their computers, but also as powerful stand-alone computers. As such, information processing has evolved well beyond the traditional central environment to distributed or decentralized operations. This trend has offered substantial benefits in productivity, customization, and information access. However, it is also meant that those control procedures, previously limited to the central operations, must be re-applied and extended to the "end-user" level.

Technology, using microcomputers as end-user computing devices, has taken data processing out of the centralized control environment and introduced the computer related risks in new areas of the banks. However, the implementation of these new information delivery and processing networks has outpaced the implementation of controls. Basic controls and supervision of these computer activities often have not been introduced, or expected, at the end-user level. The technological advantages, expediency, and cost benefits of end-user computing have been the primary focus. Recognition of the increased exposures and the demands for expanded information processing controls has lagged. These concerns for data protection and controlled operations within the end-user environments must be addressed to minimize risks from incorrect management decisions, improper disclosure of information, computer-fraud, financial loss, competitive disadvantage, and legal or regulatory problems.

End-user computing is recognized as a productive and appropriate operational activity. However control policies for data security and computer operations, consistent with those for centralized information processing functions, need to address the additional risks represented in the end-user computing operations.
Microcomputers, in the end-user computing operations, are being used basically for three purposes: 

i. as word processors,  
ii. as communications terminals with other computers (to transmit or receive information in their databases), and  
iii. as stand-alone computing  

These three functions require different control objectives, based on the risks associated with the activity. Each function requires certain operational type controls such as physical security, logical security, and the file backup. However, the more pronounced risks involve those operations using microcomputers as stand-alone processors.  

While word processing and terminal communications also require strong controls, programming/support for the operating software and applications systems generally remain centralized or is a vendor responsibility. In end-user computing, the user is often engaged in program development, in addition to information processing. This may involve the creation of programmed software from an original design or building customized routines from specialized vendor software. Regardless, the control techniques for the programming, it’s testing, and its documentation are necessary to ensure the integrity of the software and the production of accurate data.  

There are basic controls which should be present in any level of computer operations. These controls should already be present at the centralized data center. The evolution of microcomputer based systems has not eliminated the need for these basic controls, but has shifted the focus of control to the end-user level.  

Some of these basic control standards that need to be implemented in microcomputer-based systems are:  

Control requirements for microcomputer use need to be addressed by management in its internal policies and procedures. Policies and procedures should be in writing and should define what steps are to be taken to protect the bank to monitor microcomputer system acquisition and use. The purpose of this function should be to help prevent redundant uses of microcomputer systems and to ensure that there is the required degree of compatibility among hardware and software systems in use throughout the bank.  

For program development and testing, before a new system is developed or purchased, the user should have a clear understanding of the specific needs being addressed by the proposed new system.
Alternatives should be reviewed by the user and analyst to ensure that the best solution is selected. Development should be done with the aim of producing a system that is easily modified and maintained by someone other than the original developer. Finally, the completed system should be subject to rigorous testing to provide assurance that the results produced are valid and reliable.

Just as with larger systems, microcomputer systems must be adapted to meet changing requirements and circumstances. Modified programs should be subject to many of the same controls as newly-developed systems. Most important among these is the requirement that there may be a thorough testing of the modified system. In addition, accurate records should be maintained describing the change, the reasons for the change, and the person responsible for making the change.

Documentation is a potential problem in microcomputer-based systems. There is a tendency for these systems to be highly personalized, with one person fully responsible for the development, testing, implementation, and operation of a set of programs. The successful use of a microcomputer-based system and the production of specialized data may depend on the continued presence of this one person. An adequate level of documentation helps to prevent an over reliance on the knowledge of only one person. This is particularly needed when revisions to programs are required. Documentation standards should define acceptable levels of program, operations, and user documentation. In addition, there should be an enforcement mechanism to guarantee compliance with standards.

The development or purchase of microcomputer systems should be done with adequate attention given to the need for data editing routines. These routines are important to help ensure that data entering system is error-free and not likely to result in erroneous output. This control is important whether the data is being manually entered into the microcomputer or electronically transferred or "downloaded" from another system. In the case of data being "uploaded" to a mainframe, additional controls may be required at that level to guarantee the integrity of the data being transferred.

Microcomputer systems that are used for the processing of information with a direct monetary impact on the bank or its customers may require that additional data controls be established. At a minimum, these controls may include the requirement that there be a segregation of duties between the input of information and the review of that information in processed form. This control may be extended to require that a formal reconcilement be done by the reviewer of the processed information. In more sensitive situations with a significant dollar impact, there may be a requirement that certain functions be performed under dual control. The need for these types of input and output controls should be established during the early stages of program development. These special requirements need to be described in detail in the program documentation package.
The location of microcomputer systems outside of a physically-secure data center can permit unauthorized access to programs and data files used on these systems. The use of physical access restrictions complements the logical access restrictions discussed below. Basic steps would include the secure storage of diskettes or other magnetic media containing the programs and data for a particular system. In addition, since documentation on what a system does and how it is being used can provide important information that can be used to compromise system security, this information should also be secured. Finally, there should be adequate restrictions over physical access to the hardware itself, so that it is protected from unauthorized use, vandalism, and theft.

Just as in larger application systems, the need exists to identify those individuals who will be permitted access to the microcomputer system’s capabilities. In addition, there may be the need to differentiate between functions allowed for certain individuals, ranging from an inquiry capability for many persons to an override and correction capability for a few supervisory personnel. Normally, these restrictions will be in the form of password controls. Standard password-related control procedures, such as frequent changes and reporting of exception conditions need to be established to provide for effective access restrictions.

For each operational system, adequate plans should be made and precautions taken to ensure that users can adequately recover from damage to the hardware, software, and data. For some systems, an inability to process during recovery may mean that work can be held for later processing. For other systems, a manual backup may be appropriate. For some time critical, highly automated systems, arrangements may have to be made for data reconstruction or for processing on other hardware. At a minimum, for all systems, there should be secure and remote backup storage of data files and programs. Beyond this, the backup and contingency requirements for individual systems may differ and need to be addressed separately.

The audit areas should serve as an independent control reviewing microcomputer use throughout the bank. Audit involvement in microcomputer systems may begin at a general level with a review for compliance with the internal policies and procedures discussed above and may extend to detailed testing in particular areas such as the use of logical access controls. Audit procedures should be expanded to provide for adequate coverage of microcomputer systems. Responsibility for microcomputer auditing should be clearly assigned and plans for microcomputer audits should be built into the audit schedule.

It should be recognized that this list of controls is not all inclusive of methods to manage risk. Each computer operation, whether centralized or end-user, possesses different characteristics and possibly
some specialized risks. Control practices must be sufficient to minimize such risks. These recommended control features are considered fundamental to sound information processing.

In addition to the programming activity, the end-user environment supports computer processing, which may be totally separate from centralized controls. Information can be downloaded from the main databases and reprocessed by the end-user. Data can also be originated for processing in this structure. Regardless of the source, the resulting information is relied on by management for decisions impacting corporate strategies and customer relationships. The integrity of the data becomes no less important than had the data been produced through more sophisticated computer processes. Likewise, the need for control at the micro level remains equally important.

The failure to properly implement a uniform set of controls on the end-user microcomputers, consistent with those controls required in a main data-center, can create two broad categories of risks:

i. the corruption or loss of data and/or program software, and
ii. impediments to the efficient operation and management of the bank.

The quality of data is paramount to the successful management of any institution. Should the data, or the systems which produce that data, be corrupted, whether intentionally or unintentionally, financial loss is highly probable. Data corruption could result from three basic causes: error, fraud, or system malfunction.

In addition to accuracy, management requires the timely availability of data, inefficiencies, caused by poor operational controls, can further impede the production of information and result in financial loss. Regardless of the source, poor quality information and operations can adversely impact the bank in a number of ways such as (i) managerial ineffectiveness – inaccurate or incomplete data can adversely influence bank management decisions. Delays in information availability can also adversely impact corporate strategies, (ii) inadvertent disclosure – human error, fraud, or system malfunction may result in proprietary bank data, customer data, or program software being disclosed to unauthorized persons, (iii) competitive disadvantage – problems in the production of accurate and timely information can place the bank at a competitive disadvantage. Delivery of services, customer confidence, and management decisions could be impaired, (iv) legal problems – errors in the production of data or wrongful disclosure of data may result in legal actions against the bank by its customers, consumer groups, competitors, and regulators, (v) regulatory problem – failure to produce timely and accurate data can cause the bank to be in violation of regulatory requirements, subjecting the bank to regulatory penalties, (vi) monetary losses to the bank can arise from deliberate
manipulation of the data (fraud), missing or erroneous data (leading to costly incorrect decisions), or various inefficiencies in the operation of the system.

Bank management should be encouraged to evaluate the associated risks with its end-user computing networks and other forms of distributed computer operations. Control practices and responsibilities to manage these activities should be incorporated into an overall corporate information security policy. Such a policy should address areas such as management controls, data security, documentation, data/file storage and backups, systems and data integrity, contingency plans, audit responsibility, and training.

It is the responsibility of the Board of Directors to ensure that appropriate corporate policies, which identify management responsibilities and control practices for all areas of information processing activities, has been established. The existence of such a “corporate information security policy”, the adequacy of its standards, and the management supervision of such activities should be evaluated by the IT-auditors of the central bank of the country (RBI) during the supervisory reviews of the banks.

7.6 Contingency Planning for Banks and FIs
The Board of Directors and management of each bank and FI, need to ensure contingency planning for their institution. This includes both institutions that provide their own information processing service and those that receive processing or services from service-providers. This also addresses issues which should be considered when developing a viable contingency plan.

Contingency planning is the process of identifying risks from disruption of operations and services. The objectives are to minimize disruptions of service to the institution and its customers, minimize financial loss, and, ensure a timely resumption of operations in the event of a disaster.

Many banks and service bureaus have not sufficiently addressed the risks associated with the loss or extended disruption of business operations. More specifically, many contingency plans do not address all of the critical functions throughout the bank. The banks have not established or coordinated effective contingency planning efforts with their service bureaus. Many service bureaus have not established contingency plans. Often contingency plans have not been adequately tested.

The board of directors and senior management of the banks are responsible for establishing policies, procedures and responsibilities for comprehensive contingency planning, reviewing and approving the institution’s contingency plans annually, documenting such reviews in board minutes.
If the bank receives information processing from a service bureau, management must also evaluate the adequacy of contingency plans for its service bureau, ensure that the institution's contingency plan is compatible with its service bureaus.

### 7.7 IT Service Contracts

This section identifies the potential risks in contracting for IT-services and/or failing to properly account for certain contract provisions.

Most of the banks and financial institutions are entering into IT servicing contracts that contain provisions which may adversely affect the institution. Contract provisions may include extended terms, significant increase in costs after the first few years, and/or substantial cancellation penalties.

In addition, some service contracts improperly offer inducements that allow an institution to retain or increase capital by deferring losses on the disposition of assets or avoiding expense recognition for current charges. Institutions experiencing earnings and capital problems are particularly attracted to these inducements.

Examples of inducements include the service purchasing assets (e.g., computer equipment or foreclosed real estate) at book value, which exceeds current market value; the service provider making available capital by purchasing stock from the institution; the service provider giving cash bonuses to the institution once the conversion process is complete; and the institution deferring expenses for conversion costs or processing fees under the terms of a lease or licensing contract.

These inducements offer a short-term benefit to the institution. However, the service provider usually recoups its costs by charging a premium for the data processing services it provides. These excessive data processing fees adversely affect an institution's financial condition over the long-term. Furthermore, the institution's accounting for such inducements typically is inconsistent with generally accepted accounting principles (GAAP) and regulatory reporting requirements.

When negotiating contracts, an institution must ensure that the service-provider can provide a level of service that meets the needs of the institution over the life of the contract. It is also the responsibility of the institution to ensure that contracts are accounted for in accordance with GAAP (Generally Accepted Accounting Practices).

Banks also have potential risks associated with contracting long term for IT-service with independent service-providers, vendors of hardware and software, and facilities management groups.
Historically, banks have contracted for IT-services for relatively short periods of time. To stabilize costs and improve earnings, some banks had also signed longer-term contracts.

Vendors of data processing services commonly use standard contracts for their products and services. These contracts may be general, especially concerning service-provider responsibilities, and may not always protect the financial institution.

Bank management should carefully consider retaining legal counsel to ensure that both parties’ responsibilities are specified and that the bank is adequately protected. When negotiating contracts (i) do not rely on oral claims and promises; (ii) require access to the vendor’s source code and maintenance documentation via escrow agreements for turnkey operations; (iii) ensure the existing service-provider provides necessary levels of transition assistance when you convert to other automation alternatives; (iv) include cancellation, termination, and bankruptcy clauses in the contract; (v) establish ownership of and transitional access to automated records; (vi) provide financial information on a regular basis to apprise the bank of the service-provider's condition; (vii) establish a way to develop and test contingency plans; and (viii) explicitly detail audit responsibilities.

In summary, contracting for excessive servicing fees and/or failing to properly account for such transactions is considered an unsafe and unsound practice. Servicing agreements that include contract provisions or inducements similar to those discussed above should be closely reviewed by the institution. Institutions must ensure that accounting under such agreements reflects the “substance” of the transaction, not merely the “form.”

7.8 IT Risks in Mergers and Acquisitions

In the recent past world over, mergers and acquisitions within the financial industry have begun, to enhance asset growth, gain market penetration, and to achieve a competitive advantage over rival institutions. In India also it can happen in the near future.

Historically, financial institutions have acquired significantly smaller institutions and have integrated the acquired institution into an existing organizational structure. In the past several years, financial institution regulators have seen the consummation of mergers and acquisitions which have necessitated the development of new and complex information systems. One result is the consolidation of data processing systems and back office operations.

While a merger or acquisition may require the financial institution to engage in a system conversion, it should be noted that many conversions are unrelated to mergers or acquisitions. While there are
risks associated with any conversion, well managed strong institutions have generally been able to overcome conversion problems. Financial institutions have encountered unanticipated problems in the conversion process that have had implications throughout the institution. These include an adverse impact on profitability; the reporting of inaccurate financial information to regulatory agencies; the inability to reconcile general ledger accounts; management decisions based on inaccurate information; and a negative impact on public confidence.

Few cases involving conversion-related data processing problems include:

(i) a large money center bank was unable to complete processing for 32,000 trades of government securities, resulting in an overdraft of $32 billion at the Federal Reserve;

(ii) a large holding company experienced a $4 billion out-of-balance condition following a change in its transaction processing system;

(iii) as a result of a faulty general ledger system conversion, a thrift institution chronically filed late and inaccurate regulatory reports, resulting in civil money penalties being assessed; and

(iv) as the result of a faulty check processing system conversion, a thrift institution was forced to charge off unresolved book-keeping differences equivalent to one year's net income.

Poorly planned mergers have also resulted in systems conversions that have extended beyond projected time frames, resulting in unanticipated expenses and/or unrealized cost savings. Traditionally, mergers and acquisitions were accomplished within the existing systems and, with adequate pre-planning, were effected in a short period of time. In the current merger and acquisition environment, where mergers of equal size institutions are not uncommon, the potential for an unsuccessful conversion is greatly increased.

A 1989 survey by Ernst & Young and Keefe, Bruyette & Woods, Inc. of 34 banks and bank holding companies with assets over $6 billion which were involved in mergers and acquisitions showed that in mergers of equals, neither bank had the capacity to absorb the data processing and back office operations of the other. Additionally, in this type of transaction, institutions have been able to reduce data processing and operations expense by amounts substantially below projections. The survey also showed that most of the institutions had extensive experience with acquiring smaller financial institutions while only a few had been involved in a merger with another large financial institution.

The factors which increase the potential for an unsuccessful or problem conversion are insufficiency detailed plans; failure to commit necessary resources; failure to retain personnel necessary to effect a successful conversion; inadequate controls which result in reconcilement and system problems; and inaccurate reports produced by information systems.
To minimize the risks associated with mergers and acquisition involving conversions of information systems, regulators should (i) determine the impact of these activities on IT and other examination strategies. Examples of significant IT conversions include: major application changes, initial conversion to in house operations, outsourcing major applications, operating systems enhancements, and data security revisions; (ii) review the institution's IT plans for effecting the merger or acquisition as part of the application process; and (iii) monitor the status of merger and acquisition activities involving data centers under their supervisory authority.

IT services in the present context of the financial services are not complete unless they meet customer demands related to anywhere, anytime banking. One of the ways of providing this is through networking IT platforms and systems locally and globally.

7.9 Network Services and EFT Systems

A switch is a computer system that facilitates the transfer of electronic messages between terminal devices and the appropriate network participants. For example, it transmits an inquiry or transaction from an automated teller machine (ATM) or point-of-sale (POS) terminal to the depository institution that holds the customer's account. EFT terminals, processors, and switches can be configured in many different ways, depending on the participants' needs. The combination of interconnected terminals and computers is a network. Networks are sometimes operated by independent third party service providers.

Financial institutions have increased the use of switch and network services to lower costs and improve competitive position. Many financial institutions are sharing resources or using outside service providers, including non-financial companies, to provide EFT services. Such services include POS, ATM, and bill payment. Industry marketing efforts are promoting additional shared retail services, such as electronic clearings, stored value cards, and credit card authorization.

EFT switches and network processing systems have expanded traditional methods of consumer banking, e.g., deposit, withdrawal, and obtaining credit. These systems provide customers with regional or nationwide access to their funds.

Some banks are required to share these services. Others voluntarily share them on a regional, national, or international basis.

Examples of shared EFT switch and network services include a multi-bank holding company network servicing affiliated institutions; a network formed and shared by different types of financial
institutions; and regardless of the types of services offered or systems being used, there are inherent risks in switch and network services.

The increasing use of switches and networks raises certain issues (i) operational failure - system failure or service interruption, which may be caused by a disaster, could impact all connected financial institutions and could cause an erosion of consumer confidence; (ii) settlement failure - network participants could fail to make required settlement payment, resulting in significant financial losses; or, the processor could fail to provide necessary settlement records, forcing participants to reconstruct transactions; (iii) financial failure - the switch service-provider could expense sudden financial problems that may adversely impact all connected financial institutions; (iv) amount limits - the network’s amount limits, such as those applied to withdrawal, may be different from the limits the institution established; (v) audit coverage - audits may not sufficiently cover internal controls, enforcement of standards, and review of transactions processed; (vi) contracts - poorly written contracts may inadequately define participants’ liabilities and responsibilities and expose financial institutions to potential loss.

The Board of Directors and senior management of the banks should be responsible for (i) ensuring that controls covering the switch processing environment are adequate. Alternatives to accomplish this objective include qualified internal or external auditors, or consultants specializing in this area. The results of these evaluations, and management’s efforts toward correction, need to be documented in Board minutes, (ii) ensuring that contracts for switches and network services are reviewed by legal counsel and meet minimum regulatory contract servicing guidelines, (iii) ensuring that settlement procedures do not pose undue risk to their institutions and that network rules adequately address actions that would be taken in the event that a participating institution fails to settle.

Given below are the controls that should be in place in an EFT switch or network services environment.

Control for a safe and sound EFT network switching environment should address the following items. These objectives apply to all EFT switches and network services regardless of ownership.

Management should ensure (i) written, approved, and enforced policies and procedures covering personnel, security controls, operations, and disaster recovery, (ii) adequate segregation of duties and responsibilities; (iii) periodic control evaluations of the switch and network; (iv) daily settlement of switch activity and balancing of network activity, and periodic verification of fee distribution; (v) contracts that identify the responsibility and liability of all parties (e.g., timely presentation of
returned items and appropriateness of fees and surcharges); and (vi) adequate fidelity and business interruption insurance.

Security concerns of EFT should have physical access restrictions, encryption of critical data elements (e.g., personal identification code), adequate management of encryption keys used in software, Software access controls including the program library, data files, and the network, controlled access to positive and negative card files, used to authorize transactions; and institution control files (ICF) or institution parameter blocks (IPB), used to store institution specific processing criteria, and captured card procedures.

Operations of EFT must have file backup and disaster planning including telecommunications, audit trails sufficient to trace transactions through the system, stand-in processing (having the cardholder data available at the switch for authorization) procedures should be available in the event of processor downtime, including the handling of positive balance files (PBF) and cardholder authorization systems (CAS), restart and recovery procedures to ensure the continuity of transaction processing in the appropriate sequence, control over the embossing, encoding and distribution of access devices, and controls over the generation of cardholder Personal Identification Codes (PIC) and communication of PICs to cardholders.

7.10 Systems Development Life Cycle
These problems are preventable. Techniques exist to complete complex system projects on schedule, within budget and meet design specifications. These techniques are System Development Life Cycle (SDLC). Life cycle methodologies are available from vendors. Banks may also develop the process internally.

Banks implementing purchased packages as well as systems developed in-house can use these processes. SDLC methods vary but usually include procedures for conducting needs analysis, defining technical specifications, systems design, programming and testing, conversion, and; post implementation reviews, testing new or modified systems is an extremely important step. It is not prudent to install a new system before testing its full capabilities. Consideration of parallel run is also important as unresolved problems may require reverting to the previous system.

7.11 Evaluation of Purchased/Outsourced Software
In recent years, there has been an increase in the number of companies developing and marketing software systems to meet the data processing and information needs of the thrift industry. Software packages can be obtained from a variety of sources such as large IT system manufacturers, software vendors – domestic or international, etc.
There are potential risks and control issues that should be addressed when institutions consider the purchase of software systems. Some institutions have found that software does not work as expected, is not adequately supported by the vendor, or requires costly changes in existing data processing systems that were not identified prior to purchasing the software. These situations can occur if the institution lacks management guidelines for evaluating software packages or if it does not have the expertise to perform these evaluations.

For example, poorly defined user requirements may result in the selection of software that does not meet the needs of the institution, or a weak cost-benefits analysis may not identify all direct and indirect costs of installing a software package. In other cases, an ineffective financial analysis may fail to evaluate the capability of the company to support the software after installation. As a result of these and other weaknesses, institutions can incur significant costs for software or hardware modifications that were not considered or brought to light in the evaluation process. In some instances, institutions have elected not to implement newly purchased software, resulting in a monetary loss to the institution.

The board of directors and management are responsible for ensuring that policies and procedures are in place and that resources are available to properly evaluate the risks and control issues of purchased software and vendor companies prior to purchase.

The following suggestions are provided to assist management in evaluating software packages and vendor companies prior to purchasing software. They are recommended for significant software purchases or when the software will support critical aspects of the institution’s operations. These guidelines identify the type of studies or analyses that should generally be performed to improve the evaluation process and reduce the risk of the software not meeting the needs of the institution. In cases where there are limited alternatives for purchasing software such as single vendor applications, or operating system software designed for selected manufacturer’s hardware, portions of the guidelines may not be applicable.

It is generally appropriate to analyze user requirements before evaluating vendor software packages. This analysis should usually define the business reason for purchasing software, deficiencies of the current system, user and data processing requirements, user and management reporting requirements, system interfaces to other systems, and the in-house resources needed to install and maintain the system. User, Data Processing, and the Audit Departments should generally be involved in this analysis. The resulting document will provide a basis for evaluating vendor software packages.
After the user requirements analysis is completed, the direct and indirect costs of installing and maintaining purchased software should be compared to other business alternatives such as the use of service bureaus, modifications to existing applications, or manual systems. The capabilities and costs of each alternative should be analyzed and compared in a common format. The purchased software alternative should include the costs of modifications to existing data processing systems and expected return on investment.

If the results of the user requirements analysis and cost-benefit study indicate purchased software is cost-effective and the preferred solution, the following factors should be evaluated.

The financial statements and resources of the software-company should be analyzed to determine whether the company is financially sound and has the resources to support and maintain the software package during its estimated life span. This analysis is especially important if the vendor is responsible for future modifications to the software programs. In these cases, procedures should be established to analyze the financial statements, performance, and stability of the company on annual basis.

The software company’s contract should be carefully reviewed by appropriate management and legal personnel to identify potential risks for the institution. This review should identify the contract deliverables, scheduled delivery dates, method of delivery, documentation, and other key contract terms. It should also include the obligations of the software company to support the software after purchase, furnish updates, and arrange for supplying the program source code and documentation if the software company goes out of business. The provisions for terminating or extending the contract should be clearly spelled out. Recourse for monetary losses as a direct result of errors in the software should also be considered. Requirements for annual financial information, preferably audited, should be incorporated into the contract.

The banks making a substantial investment in new software should consider including in the contract the right of their internal IT-auditors and also external IT-auditors (including RBI-auditors) to perform IT-Audits/Inspections of the software companies for risk and control issues relating to the software purchase by the banks.

User references are an important source of information in evaluating vendor packages. A user reference list of other institutions using the software package should be obtained from the vendor. These companies should be contacted to obtain information such as the software package purchased, the computer system used to run the software, modifications that were made after installation, the
length of time in use, the quality of vendor conversion support, performance on similar hardware, and other pertinent information.

Visits to other institutions which have installed the software on a similar computer system should be considered before making a substantial investment in a software package. Care should also be taken in purchasing software that has not been installed and thoroughly tested in other locations.

The software package should be reviewed for security controls and audit trails such as access to data files, authorizations, password controls, data access logs, reporting of security violations, and capabilities of utility programs to alter data.

The age of the software, the number of updates issued since it was developed, the software vendor’s plans for future modifications, and the useful life of the package should be evaluated against the institution’s short-and long-term business plans.

The documentation and manuals provided with the software package, and on-line help programs if the system is interactive, should be carefully reviewed by Data Processing and User Departments for content, readability, and completeness. This review should include input forms and output reports, compliance with in-house standards, and documentation provided with modifications.

Vendors should test all parts of the system in a systematic manner. Information on the testing procedures performed by the vendor should be obtained and evaluated. This information should include test plans, the hardware used for testing, and the method used to verify that the software calculations meet regulatory requirements e.g., Truth In lending disclosure calculations.

The background and experience level of software company personnel assisting the institution in conversion planning, support, and training activities should be obtained and evaluated. The vendor should provide a detailed schedule of pre and post conversion support activities with associated costs. Conversion support materials should be carefully reviewed for quality, readability and completeness. The software company internal resources required to support conversion training should also be evaluated. The quality of conversion support provided by the vendor should be verified when checking user references.

The capability of the vendor company to provide timely, on-going maintenance support for user programming requests, product updates and regulatory changes should be evaluated. The content, frequency and costs of previously issued software updates should be reviewed. The software should also be evaluated for report-writing capabilities that permit in-house personnel to produce new or
specialized reports for management, user departments, or to comply with regulatory requirements. If vendor programming is required for report modifications, these costs should be considered in the evaluation.

After evaluation and selection of a software package that meets the needs of the institution, the software contract should be approved by senior management. Management should provide for an effective project control system to facilitate planning and implementation of the software. Liaison personnel should also be designated to manage the vendor relationship and coordinate the software installation.

7.12 Conclusion

Various issues identified and the suggestions given here based on empirical work reported in Chapter 5, are used to evolve a new framework for IT-audit-based IT-Risk Rating/Management System which is discussed in Chapter 8.