Chapter 1

Computer Security, Audit and Controls:
Concept and Review of Literature
Chapter 1

Computer Security, Audit and Controls:
Concept and Review of Literature

1.1 Introduction
This decade has witnessed an explosion in computing and communication capabilities. These technological advances will continue even with greater speed to increase our ability to acquire, store, process and network the data. As a result, more and more information is being (and will get) shared in day-to-day functions of banks, making Information Technology (IT) the very lifeblood of banking. Hence, the issues related to security, audit and control can never be overlooked. These issues related to computer hardware, systems software, application software, data and its communication should all be considered in a holistic manner.

1.2 Hypothesis and Objectives of the Study
The hypothesis of the present study is as follows:
Wherever computer-audit is being done effectively, the chances of occurring computer-frauds/irregularities are less. And wherever it is not being used effectively, the chances of occurring computer-frauds / irregularities are high. Thus, there is a direct relationship between the computer audit and control over frauds/irregularities in the computerised environment. That is, computer-audit keeps a check on possible irregularities, malpractices and frauds in computerised environment. The adequate internal controls through computer-audit make the computer-based business operations secure and smooth. Reverse is the case where in computer-audit is not done.

And, the Objectives are:
1. To identify the gaps in the literature relating to computer audit with reference to computerised banks in India.
2. To study the working of the selected bank-branches in computerised environment from the point of view of computer-audit, detection and prevention of frauds/irregularities etc., through computer-fraud risk assessment exercise.
3. To collect the cases on computer-security breakdowns, and to prepare success case/s on and the use of computer-audit in bank-branches, for creating awareness among the top management.
4. To workout and suggest appropriate strategies for conducting computer-audit, and
5. Finally, offer suggestions on improving deficiencies in computer security and audit-
related areas in banks in India.

1.3 Computer Security

Today, survival of the bank is often dependent on the quality, adequacy, and integrity of its
information. Protecting information and the infrastructure that processes and maintains this
information becomes critical to the continuity of the business-operations. The health of the
bank is often directly influenced by the health of its information, and the health of the
information is dependent on the health of the underlying hardware and software systems
(including the health of the application-software systems). Thus, the need for the “protection”
or “security” must embrace basic health (i.e. adequacy, integrity, quality, accessibility etc.) as
well as responding to and averting threats. Security of information-resources must include
controls and safeguards to offset possible threats as well as controls to ensure timeliness,
availability, integrity, and other measures of robustness, or “health”.

Therefore, computer-security may be defined as (1) controls to ensure the continuity of
adequate information and (2) protection of computing & communications assets i.e. IT and IS
(Information System) assets from loss/damage as also to ensure the controls in order to avoid
unauthorised access to IT and IS. As a logical extension, the avoidance of loss or damage to
other assets through information inadequacy or through abuse or misuse of computer facilities
should also be within the scope of “Computer Security”.

1.4 Computer Audit

Management should use the audit function as an independent arbiter to measure compliance
with policies, standards, and guidelines as well as to assess the adequacy of information
security. Management must concern itself with safeguarding the information resources under
its jurisdiction.

Computer Audit (sometimes it is also called as Electronic Data Processing Audit i.e. EDP
Audit or Information Technology Audit i.e. IT-Audit or Information-Systems Audit i.e. IS
Audit), assumes greater importance in the context of accelerated pace of computerisation
taking place in Indian banking sector. Even though computerisation leads to improvement in
customer service, housekeeping, productivity and profitability, it need not be construed as a
panacea for all the problems being faced by the banking industry, or its implementation is not
going to be without attendant problems or areas of concern. Uncontrolled use of computer can
cause loss of important data. Inaccurate or untimely data can lead to incorrect decision-making. Computer abuses/frauds caused by outsiders or employees can land the bank in serious trouble and in the absence of any vigilant machinery, detection of computer frauds/abuses can be left to chance. Protecting the IT related assets viz. hardware, software and data is of vital importance. Computer error can prove to be costly in the long run and loss of confidential data can attract claims for compensation. Hence, there was urgent need felt for banks to have IT systems with proper audit/control over such systems.

Computer Audit could be defined as a process of collecting and evaluating evidence to
1) determine whether a computer system could safeguard assets through adoption of adequate security and control measures,
2) maintain data integrity, achieve the goals of the organisation effectively, and
3) result in efficient use of resources available. Data integrity implies that data having certain attributes like completeness, accuracy, timeliness, effectiveness and reliability are consistently maintained during input, processing, storage, retrieval and communications.

1.5 Controls in IT environment

Every bank and FI should identify the events and circumstances whose occurrence could result in a loss to that organisation. These are called exposures. Controls are those acts which the organisation should implement to minimise the exposures. In addition to knowing the cause(s) of exposure that a particular control is intended to act upon, it is also useful to know the type of role the control is intended to perform. There are basically four categories of control:

Deterrent: These controls are designed to deter people (internal as well as external to the organisation) from undesirable behaviour. For example, written policies to deter people from doing undesired activities.

Preventive: These controls prevent the cause of exposure from occurring, or at least minimise the possibility. For example, security-controls at various levels like hardware, system software, application software, database, network etc.

Detective: When a cause of exposure has occurred, detective controls report its existence in an effort to minimise the extent of the damage. Certain fire precautions (such as heat detectors, smoke detectors etc.) fall into this category. Even auditing function can many times be also treated as a detective control.

Corrective: These controls are necessary to recover from a loss situation. For example, without corrective controls in place (in the form of Disaster Recovery Management System),
the bank has risk of loss of business and other losses (which could even result in bank going out of business) due to its inability to recover essential IT-based services, information and other resources, after the disaster strikes.

1.6 Review of Literature

The following review of literature about the subject shows the importance of computer audit, security and controls.

In view of the need felt to review the internal controls, inspection and audit system in banks in India, the RBI (Reserve Bank of India) had constituted a Working Group (in 1995) under the Chairmanship of Shri Rashid Jilani, the then Chairman and M.D., Punjab National Bank. And, one of the focus areas of this committee was Computer Audit. The Committee has given a number suggestions, a gist of which is given in chapter 4 “Computerisation and Computer-audit in Banks in India”.

The Committee on Banking Sector Reforms (Narasimham Committee – II) has in the Report dealt with, in detail, the issues in technology upgradation, and observed that most of the technologies that could be considered suitable for India have been introduced in some form or the other as a pilot. The desired success has not, however, been achieved. (The committee also dealt with the systems and procedures in the computerised environment and re-emphasised the importance of effective computer-audit procedures in the Indian banking industry) (2).

In 1999, the Reserve Bank of India had published a report of a Committee appointed to examine various issues pertaining to technology upgradation in the banking and financial sector, and to suggest steps for time-bound implementation schedule of the Narasimham (II) Committee’s recommendations. This committee also felt the need for strengthening the IT-audit and security procedures in the banks in India.

In the report (1999) of the Study Group on Large Value Bank Frauds, appointed by the RBI, the study-group has rightly recommended that the banks should evaluate the risks inherent in computerised and telecommunications banking, and place adequate control mechanism for these risks.

The book “Managing Technology in Financial Institutions”, {James Essinger, Financial Times – Pitman}, gives practical guidance on the deployment of financial technology, and
information about how to manage it. It draws together current thinking and best practice in deploying financial technology and shows how to use computer technology as a tool to gain competitive edge, provides step-by-step guide to implement a new technology application, examines the fundamental elements of financial technology, surveys all major real-life applications of financial technology, and emphasizes the importance of planning and deploying computer-security related precautionary measures. It also examines the future deployment of financial technology and the range of possibilities open to the financial markets by giving a wide range of international examples.

Another book, “Management Handbook of Computer Operations”, {Gordon Longworth, NCC Publications} was also referred during this study. The main focus of this handbook/manual is to assist in the definition of installation-based standards for activities concerned with the provision of operational computing facilities. This book also includes Data Processing Documentation Standards, Standards in Programming, Project Planning and Control, Computer Security & Controls etc.

The book “EDP Auditing - A Functional Approach”, {Albert J. Harnois, Prentice-Hall International }, is a practical guide to EDP auditing. Its functional organization makes it much more than just a valuable reference manual. It is designed as a working tool for experienced internal EDP auditors. This book provides valuable information on issues such as : Effectively Using Mainframe Data Security Software. It also covers the administrative procedures such as, establishing the EDP audit function, determining which reviews to perform and when, and administering an established function. The EDP auditing procedures such as performing general controls reviews, performing reviews of existing computer applications, performing system development reviews, performing system acquisition reviews, tackling the systems software reviews, evaluating PC controls, conducting a database review, evaluating and effectively utilizing mainframe data security software, change control systems, developing and using computer audit software, are covered in this book. Using and reviewing expert systems is also covered in the book.

The “Computer Security Reference Book”, {ed. K M Jackson & J. Hruska, Butterworth Heinemann, 1992}, is a comprehensive reference book that provides an in-depth treatment of the whole field of computer security including computer crime, data protection, EFTPOS schemes, evaluation of security products, hacking, risk analysis, telecommunications, Unix security, viruses, access controls, ATMs (Automated Teller Machines), building secure systems, computer fraud, contingency planning, copy protection, data protection, distributed systems, document security, encryption algorithms, legal aspects of computer security, multi-
level security and trusted systems, network-security in banking, security in hardware and software form, international standards in computer security, and many other important aspects of computer security.

The financial services industry is experiencing increasing competitive and cost pressures. There is a need to maintain and develop a quality service whilst continuing to improve efficiency. The book, “Managing for Quality in the Financial Services Industry”, {Tony Ansell, Chapman & Hall, 1993}, is a detailed reference manual which explains the key techniques of quality management and their practical application in banking and financial institutions. It describes how to introduce a quality culture at all levels ranging from the top management introducing an organization-wide total quality programme, for improving and maintaining quality standards in branches. Quality management involves a wide range of specific management techniques such as identifying customers' requirements, problem analysis, introducing quality management information, designing quality, training and motivation, process analysis, contingency planning etc., all this is explained in a lucid language in this book.

Effective internal audit is an invaluable tool of modern management, providing positive assurance on the effectiveness and adequacy of control in a changing environment, by identifying strengths and weaknesses and recommending any necessary remedial action. It also assists the achievement of management objectives by identifying opportunities and threats, and offering practical ideas for addressing them. The authoritative reference book, “Manual of Internal Audit Practice”, {ed. H J Stearn and K W Impey, ICSA / IIA Publishing Limited, 1996}, covers all aspects of the practice of internal auditing, with particular emphasis on the practical application of the principles involved in computer audit and prevention & detection of frauds.

The book “Computer Security” {John M Carroll, Butterworth-Heinemann}, contains few ideas on recent advances in computer hardware and software security. It includes new information on: the threats to computer security, computer crime and law, organizing for EDP security, protection of information, screening and management of personnel, physical access control, disaster prevention, control and recovery, computer communication-line security, transmission security, cryptographic security, systems security, integrity and reliability, risk management, and modes of risk analysis.

assessment and, in particular, a generalised methodology that enables the reader with a basic understanding of internal controls to prepare effective testing plans for any type of system and, more especially, for computer-based systems in view of their wide popularity in all fields of endeavour in today's world.

The IIARF (Institute of Internal Auditors' Research Foundation) had commissioned a skilled team from the University of Southern California, to determine what is expected in terms of future technological change. The team was asked to identify the future workstation and the future work environment, the evolving control environment, the future process of audit testing and, most importantly, the education and skills that will be required of the future internal auditor. This study provides significant information for the practitioners, the academic community, and business educators preparing the auditors who will work in the next century.

This report ("The Impact of Technology on Auditing - Moving into the 21st Century, Gary Holstrum, Theodore Mock, Robert West, IIARF), describes a two-phased research project designed to forecast and analyse the most significant changes in Information Technology (IT) by the year 2000 that may affect auditing. Phase I of the project developed a statement of the problem, the need for the project, a preliminary review of relevant literature, and an initial list of events, and trends that were identified as being potentially important to auditing. Phase II implemented a Delphi study to obtain estimates of when various technological (primarily computer-related) events could be expected to occur. For these events and trends that were considered likely and relevant, an attempt was made to determine their future impact on auditing. The approach used for research was as follows: The Problem (a set of problems), Objectives, Literature, Methodology, Results, Other Results. Overview of audit-implications of the research is also dealt with, by giving future auditor's tool-kit, control-environment and systems-applications, audit-testing, the changing role of auditing, future organizational structure of the audit-function, the skills required of the future auditor, and the education and training of the future auditor.

Technological advantages are occurring too fast and the internal auditors faced with the challenge of using as well as auditing these sophisticated systems need to keep up with the evolution. "Information Systems Auditing", a Collection of Articles from Internal Auditors, edited by C. Richard MacWilliams, Institute of Internal Auditors, 1996, has covered a wide range of articles in this collection. The general topics covered are: Confessions from a Computer Professional about IT-audit, An Effective Approach to EDP Auditing, importance of Documentation in IS-Control, Design of the Data Center, etc. The book also covers use of IT in Audit function itself, then Systems Development Auditing, computer security, Disaster Recovery Planning, Controlling Computer Crime, Access Control Assures Network Security,
and Perimeter Security for Telecommunication with External Entities. He has explained audit and security concerns in End User Computing activities also.

“Guidelines for Establishing an Information Systems Audit Function”, {Leta Fee Higgins, Institute of Internal Auditors, 1996}, is useful to help auditors to identify the need for information systems audits. Rather than concentrating on the technical details required for performing information systems audit, in this book it is focussed on showing how to set up the actual function for various organizations. In the past, auditors tended to view computers as being highly reliable. Computers were performing increasingly complex calculations and manipulations on business information. However, humans were programming those processes being performed by the computers and, of course, were prone to errors.

The book “Information Systems Management, Control and Audit”, {Ian A. Gilhooley, Institute of Internal Auditors, 1997}, identifies the knowledge and skills that are required to audit within the various structures of information processing systems and shows how to develop a comprehensive IS-audit approach. When this approach is used, the internal auditor is able to issue relevant and accurate reports to management on the results of individual audits. He has discussed in detail : (1) Exposures, Causes of Exposure, and Controls : Categories of Controls, the System of Internal Controls, the Impact of Information Systems on Internal Controls, defining Management's Objectives, types of Exposure, the Scope of Information Systems Controls, (2) The Audit Function : Organizing the Internal Audit Department, Staffing the Internal Audit Department, Developing an Audit Plan, The IS-Audit Process, (3) Information Systems Organization and Administration : Control Perspective, Scope of Information Systems Organization and Administration, Causes of Exposure and controls required, (4) Information Systems Security : Scope of Information Systems Security, (5) System Development, (6) System Maintenance and Change Control, (7) Information Systems Problem Management, (8) Information Systems Contingency Planning (9) Information Processing Operations, (10) Application Systems, (11) Systems Software / Environmental Control Programs, (12) Data Management, (13) Data Base Management System / Data Dictionary (14) Telecommunications Networks, and (15) Artificial Intelligence / Expert Systems. For each of these areas, the approach adopted by the author was : Control Perspective, Scope of that particular area, Skill and Knowledge Objectives (Level 1 and Level 2), Causes of Exposure, Controls required, Types of Exposures, and Audit Approach needed. He has described as to how to make an Overall Assessment of the Information Systems Function, how to conduct Systems and Acceptance Testings, how to conduct an Impact Analysis, what are the various control issues in End-User Computing (e.g. system Control Issues, Management Controls, Data Security Controls, connectivity controls,
The book “IT as a Strategic Response” {Prof. S M Padwal, National Institute of Bank Management, Pune, 1996} reviews the achievements and milestones reached in IT area till 1996 by Indian banks, gives the trends in IT, and suggests strategies that banks need to adopt to move towards their IT mission. It also suggests the Information Security Strategy encompassing analysis of risk-factors in a typical branch automation system, security requirements for fully computerised branches and also for network of branches.

The book “IT, MIS and Productivity in Banks”, {Prof. S M Padwal, Himalaya Publishing House, 1997}, explains the security and auditing of IT in banks and financial institutions. The book mentions various kinds of threats to the computer-based systems, and the various controls required to protect information and IT from these threats. He has also spelt-out the function of IT-auditing in banking.

The book “EDP Auditing - Conceptual Foundations and Practice”, {Ron Webber, Second Edition, McGraw-Hill International Editions, (MIS Series), 1988, the edition which is available in the market now}, is still (even after more than a decade) being well received by the IT-audit community and is still being considered as the standard reference on EDP-auditing. This book is divided into six parts. In the first part, author has given an overview of EDP audit function within an organization. In the second part, he has given a framework for control function of the management, the relationship between the top management and EDP management, its evaluation, System Development Life Cycle (SDLC) and the role of auditor in SDLC. He has also discussed in this section, the Programming Management, Data Resource Management, Security Administration and Operations Management. The third part deals with application controls. In this section, various types of controls like access controls, cryptographic controls, PINs (Personal Identification numbers), Digital signatures, plastic cards, audit trail controls, Data and instruction input controls, Validation and error controls, communication controls, processing controls, database controls, output controls are discussed. Part No. 4 deals with the evidence collection by using generalised audit software and other specialised audit softwares, code review technique, concurrent auditing techniques, interviews, questionnaires, and control flowcharts, performance monitoring tools etc. The next part is dedicated to the evidence evaluation. Here, the author has explained how to evaluate the safeguarding of the assets, data integrity, system effectiveness and system efficiency. In the last section, he has presented the organization structure and management of EDP audit function, besides mentioning the changes taking place in the EDP audit function. In this book, author has focussed on "controls approach" rather than on "exposures approach".
Another book “Auditing EDP Systems”, {Donald A. Watne, Peter Turney, Prentice-Hall International Editions, 1990}, has also covered the similar topics. This book is divided into four parts. Part I provides a good introduction to the topic. Part II provides an overview of computers and data processing. Internal controls required in the EDP-environment and the assessment of the existing controls are covered in detail in the Part III. The last one deals with the various techniques available to the computer auditor for testing the programs, files, and processing. The approach for auditing of the vendor-supplied systems is also explained. Expert systems can be both a tool to aid the auditor, and also they can be audited as a target of the audit; this is discussed in the last section of the book.

The book “Network Security”, {Steven L. Shaffer, Alan R. Simon, AP Professional, London, 1994}, is an attempt to bring network security out of the closet, with the specific purpose as to provide with practical approach to network security.

During the course of this study, the Year 2000 Problems were cropped up, which could have created serious problems in the computerised business environments all over the world. The Indian banking industry was not an exception to this. Therefore, in order to prevent this potential disaster in the IT environment in the Indian banking sector, the researcher anticipated the nature of this problem and started working on it well in advance way back in 1996, from various relevant angles like Management, IT-Staff, IS-Auditors, and End Users.

It was also attempted to refer various issues of journals related to the computer security, audit and control. Some of the important ones are: (a) COM-SAC Computer Security, Auditing & Control, A publication of Management Advisory Services & Publications, U.S.A., (b) CPRJ Contingency Planning & Recovery Journal, A publication of Management Advisory Services & Publications, U.S.A., (c) Network Security Journal, (d) Internal Auditor (USA). Many of the articles in these journals throw light on the topics covered above.

1.7 Conclusion

The above review of literature shows that, though there is some literature available on this topic, the most of the work done is in context of the well developed economies where IT/IS architecture and processes are well matured. The security, audit and control aspects for the organisations in transition from manual systems to computerized systems is one of the major gaps in the literature. Moreover, its relevance to Indian banking industry in general and public sector banks in particular is limited. What follows is relevant comprehensive framework for IT- security, audit and control systems in banks with particular reference to Indian Banking.
The development process of the framework is iterative one. The basic framework was prepared after studying the literature gaps from the point of view of its applicability to Indian banks. The framework was then used for auditing IT in some banks, and it was validated using empirical data of such IT-audit during last three years. The framework was again modified based on empirical work so done. The modifications and testing and re-modifying the framework is a continuous process particularly when IT is changing so fast. With reference to globalisation on one hand and financial sector reforms on the other hand, “banking” itself is undergoing a fundamental change. It is now becoming “financial services” at one-stop. The present framework reported, therefore, is not claimed as fully comprehensive one. However, the methodology used for developing the model (the framework) is such that as the changes in IT/IS on one hand and banking and financial sector on the other take place, the framework itself can be modified suitably.

The following Chapter 2 gives the conceptual framework for IT Security, audit and control systems in banks/financial institutions.

------ *** ------