CHAPTER FIVE

ANALYSIS OF EDP AUDITING SYSTEM IN BANKS
5.1. INTRODUCTION

Today, the road ahead for the banks whether conventional or Islamic is multiple and complicated, they are following their customers who want choice, convenience and control in minimum time and maximum quality in 24 hours banking service and 7 days banking work. Nowadays the globe due to the products of Electronic Data Processing (EDP) environment is the world of technology and communication and if only one bank innovates a new product, promptly other banks by their clients are asked to present such product. Due to this progress in the advanced countries, the banks in developing as well as less developed countries in where the most of the Islamic banks are running there, by their clients are requested to provide and present these facilities. Today EDP system have caused to change all aspects of our environment and banking industry has become information intensive industry and E-banking as a product of EDP system has introduced new products of modern banking services in where they can satisfy new wants of bank’s customer who are moving and they do not know any distance to catch banking products.

Therefore to handle these progress and advancements, the role of internal controls as no longer but more and more has become significant and they must cover and support security of all sections in bank’s activities, specially new banking products like Internet banking, in other words the auditing of banks in the new millennium has been involved with the new challenges, so new skills, new knowledge, new techniques, etc. have been required.

This chapter is intended to provide a background of EDP auditing system with reference to banking system through collection of a checklist for various controls related to EDP system and next to this, computer-assisted audit techniques (CAATs) as a suitable tool to
handle auditing of such system is studied. Thus this chapter is to be classified into the following sections:

5.2. EDP AUDITING SYSTEM OVERVIEW

5.2.1. EDP system definition

5.2.2. Definition of EDP auditing system

5.2.3. Auditing standards related to EDP auditing system

5.3. EDP AUDITING SYSTEM IN BANK

5.3.1. Definition of bank and its characteristics

5.3.2. Special auditing considerations in banks

5.3.3. The position of EDP system in banks

5.3.4. Internal controls in EDP system in bank

5.3.5. EDP controls in bank through Internal Control Checklist

5.4. COMPUTER-ASSISTED AUDIT TECHNIQUES (CAATs)

5.4.1. Tests of controls without (around) the computer

5.4.2. Tests of controls with (through) the computer

5.4.3. Some kinds of computer-assisted audit techniques (CAATs)

5.4.4. Generalized Audit Software (GAS)

5.4.5. Applications of GAS like ACL in bank

5.2. EDP AUDITING SYSTEM OVERVIEW

In this section, the concept of EDP system and next to this, the EDP auditing system and auditing standards relating to such system in details would be as follows discussed:

5.2.1. EDP system definition

The Electronic Data Processing (EDP) or Automated Data Processing (ADP) in initial days and Computer Information Systems (CIS) or Management Information Systems (MIS) or Information Technology (IT) in nowadays refer to a system or environment in which a computer of any type or size is utilized to process data by an organization or entity.
Jain (2001)\textsuperscript{1} says “The word computer is derived from the word ‘Compute’- which means to calculate, a computer is an electronic equipment capable of solving problems by performing complex processing of information without manual intervention at a tremendously fast speed”.

Generally a computer system consists of three major components namely (i) Central Processing Units (CPU) like main memory and control unit, (ii) Input devices like a Keyboard and (iii) Output devices like a printer. Therefore the components of an EDP system can be included as (i) Computer Hardware like Central Processing Units (CPU), Input and Output devices (ii) Computer Software like programs (iii) Methods of organisation and processing of data.

5.2.2. Definition of EDP auditing system

Weber (1988)\textsuperscript{2} “EDP auditing is a function that has been developed to assess whether computer system safeguard assets, maintain data integrity, and achieve the goals of an organisation effectively and efficiently”.

Kaveri (1996) defines that the EDP audit is a process of collecting and evaluating evidences to ensure whether the computer system provides for the safeguard of the assets through adoption of security and control measures, data integrity and optimum use of assets.\textsuperscript{3}

Accordingly EDP system through an organisation is established to process data speedy, efficiently and economically and EDP auditing is a process of gathering and assessing evidence to ensure that a computer system safeguards its assets including hardware, software,
and data by adequate auditing techniques and whether it maintains data integrity so the pre-determined objectives, set up through management could effectively and efficiently with the best use of resources achieved.

So in this regard the EDP auditor is an individual whether internal or external who performs an EDP audit within an entity to analyse and assess these above process through adequate auditing techniques including manual techniques as well as auditing software packages.

5.2.3. Auditing standards related to EDP auditing system

Basically the performance and function of an auditor is based on the nature of auditing in where it takes its regulations from standards that by some reliable financial boards such The International Auditing and Assurance Standards Board (IAASB) or American Institute of Certificate Public Accountants (AICPA) are issued. In the following these above two boards in a short review are defined and then, auditing standards related to EDP systems and banking industry issued by IAASB are shortly described. (A complete list of auditing standards issued by IAASB would be given in appendix three)

5.2.3.1. American Institute of Certificate Public Accountants (AICPA)

Keel & Boynton (1992)\(^4\) say, “The public accounting profession’s national professional organization is the AICPA. Membership in the AICPA is voluntary. Currently, there are approximately 300,000 members…. The AICPA provides a broad range of services to members including practice and quality review standards, a code of professional ethics, continuing professional

education (CPE), and technical accounting and auditing assistance. The Auditing Standards Division of the AICPA is responsible for establishing auditing standards for the public accounting profession. One arm of this division is the Auditing Standards Board (ASB), which has been designated as the senior technical body of the AICPA to issue pronouncements on auditing standards. The pronouncements of ASB are called Statements on Auditing Standards. Compliance with SASs is mandatory for AICPA members who must be prepared to justify departure from such statements. The auditing standards that are most widely recognized in the public accounting profession are called generally accepted auditing standards. These standards were originally approved by the members of the AICPA. They have been seen incorporated into the statements on auditing standards. GAAS establish the quality of performance and the overall objectives to be achieved in a financial statement audit. Accordingly, they are used by peers, regulatory agencies (such as the Securities and Exchange Commission), and courts of law in the evaluating the auditor’s work”.

5.2.3.2. The International Auditing and Assurance Standards Board

The International Auditing and Assurance Standards Board (IAASB) is a part of the International Federation of Accountants (IFAC). The International Federation of Accountants (IFAC) is the worldwide organization for the accountancy profession; Founded in 1977, its mission is to serve the public interest, strengthen the global accountancy profession and contribute to the development of strong international economies by establishing and promoting adherence to high-quality professional standards, furthering the international convergence of such standards, and speaking out on public interest issues where the profession’s expertise is most relevant. IFAC is headquartered in New York City and is staffed by accounting and other professionals from around the world. The objective of the IAASB on behalf of the IFAC Board, is to improve auditing and assurance standards and the quality and uniformity of practice
throughout the world, thereby strengthening public confidence in the global auditing profession and serving the public interest, by:
A) Establishing auditing standards and guidance for financial statement audits of such high quality that they are acceptable to investors, auditors and governments, banking regulators, securities regulators and other key stakeholders across the world.
B) Establishing high quality standards and guidance for other types of assurance services on both financial and non-financial matters.
C) Establishing standards and guidance for other related services.
D) Establishing quality control standards covering the scope of services addressed by the Board.
E) Publishing other papers on auditing and assurance matters, thereby advancing the public understanding of the roles and responsibility of professional auditors and assurance service providers.
And therefore the IAASB issues:
a) International Standards on Auditing (ISAs): ISAs are to be applied, as appropriate the standards by auditors in the audit or review of historical financial information.
b) International Standards on Assurance Engagements (ISAEs): ISAEs are to be applied as the standards in assurance engagements dealing with subject matters and information other than historical financial information.
c) International Standards on Related Services (ISRSs): ISRSs are to be applied as the standards to compilation engagements, engagements to apply agreed upon procedures to information and other related services engagement as specified by the IAASB.
d) International Standards on Quality Control (ISQCs): ISQCs are to be applied for all services falling under the standards including, ISAs, ISAEs and ISRSs.
The current membership in the IAASB consists of over 160 professional accountancy bodies in 119 countries, representing more than 2.5 million accountants in public practice, education,
government service, industry and commerce. (For more details refer to http://www.ifac.org/Guidance.)

Hayes et al. (2005) believe that “The International Auditing and Assurance Standards Board aim for voluntary international acceptance of its guidelines…. ISAs will be mandatory in Europe in 2005, and other regions in the world including the USA may follow”.

Out of total pronouncements issued by the IAASB, six pronouncements namely 401,1001,1002,1003,1008, and 1009, directly related to EDP auditing system, but IAASB because of some reasons withdrew these above standards.

IFAC (2004) announced, “The International Auditing and Assurance Standards Board (IAASB) announced the withdrawal of the following four International Auditing Practice Statements (IAPSSs):

- IAPS 1001, IT Environments - Stand-Alone Computers
- IAPS 1002, IT Environments - On-Line Computer Systems
- IAPS 1003, IT Environments - Database Systems
- IAPS 1009, Computer-Assisted Audit Techniques

At its December meeting, the IAASB concluded that the need for these IAPSSs has been superseded by the assumption of computer processing in the revised standards on understanding the business and assessing the risks of misstatement. They have also been outdated by the continuing pace of innovation in information technology. These IAPSSs have been withdrawn effective December 31, 2004. The IAASB, in a September 2004 Consultation Paper titled improving the Clarity and Structure of IAASB Standards and Related considerations for Practice Statements, describes the present role of IAPSSs, identifies matters for further consideration, and asks for respondents' views on the future role of IAPSSs”.

---

5 http://www.ifac.org/Guidance (Visited on 20,12,2005).
7 The Consultation Paper can be downloaded from the IFAC website at http://www.ifac.org/Guidance. (Visited on 15,12,2005).
Since, until now the substitutions for these above standards through the IAASB have not been declared and generally the new standards related to audit of EDP system might be stand on the basis of the previous the said standards and also to present a common view of these standards, in the following paragraphs, only the vital points of these standards in a very short review are to be expressed.

401. Auditing in a Computer Information Systems Environment

As per online handbook issued by IFAC (2004) some vital points that had been mentioned under this above standard are:
A) Computer information systems (CIS) environment exists when a computer of any type or size is involved in the processing by the entity of financial information of significance to the audit, whether that computer is operated by the entity or by a third party. (The CIS is used throughout this ISA in place of electronic data processing (EDP) used in prior ISA ‘Auditing in an EDP Environment.’ Related International Auditing Practice Statements revised and issued subsequent to this ISA use the term “information technology (IT) environments.”)

B) The auditor should consider how a CIS environment affects the audit.

C) Objective and scope of an audit does not change in a CIS environment. However, the use of a computer changes the processing, storage and communication, etc.

D) The auditor should have sufficient knowledge of the CIS to plan, direct, supervise and review the work performed.

E) The nature of the risks and the internal control characteristics in CIS environments include the following:

i) Lack of transaction trails.

ii) Uniform processing of transactions, thus the clerical errors ordinarily associated with manual processing is virtually eliminated. Conversely, programming errors (or other systematic errors in
hardware or software) will ordinarily result in all transactions being processed incorrectly.

iii) Lack of segregation of functions.

iv) Potential for errors and irregularities. The potential for human error in the development, maintenance and execution of CIS may be greater than in manual systems, partially because of the level of detail inherent in these activities.

v) Decreased human involvement in handling transactions processed by CIS can reduce the potential for observing errors and irregularities.

vi) Potential for increased management supervision.

vii) Potential for the use of computer-assisted audit techniques.

viii) Therefore both the risks and the controls introduced as a result of these characteristics of CIS have a potential impact on the auditor’s assessment of risk, and the nature, timing and extent of audit procedures.

F) The risks may result from deficiencies in pervasive CIS activities such as program development and maintenance, systems software support, operations, physical CIS security, and control over access to special privilege utility programs.

G) The risks may increase the potential for errors or fraudulent activities in specific applications, in specific databases or master files, or in specific processing activities.

H) The auditor’s specific audit objectives do not change whether accounting data is processed manually or by computer. However, the methods of applying audit procedures to gather evidence may be influenced by the methods of computer processing. The auditor can use manual audit procedures, computer-assisted audit techniques, or a combination of both to obtain sufficient evidential matter. However, in some accounting systems that use a computer for processing significant applications, it may be difficult or impossible for the
auditor to obtain certain data for inspection, inquiry, or confirmation without computer assistance.\(^8\)

**1001. IT Environments—Stand-alone Personal Computers**

As per online handbook issued by IFAC (2004) some vital points that had been mentioned under this above standard are:

A) The control considerations and the characteristics of the hardware and software are different when a PC is linked to other computers. Such situations often lead to increased risks.

B) Effective policies and procedures for the acquisition, implementation, operation and maintenance of stand-alone PCs can enhance the overall control environment. A failure to implement such policies may lead to the entity using out of date programs and to errors in the data and the information derived from them, and may lead to an increased risk of fraud. Such policies and procedures include the following:

'Acquisition, implementation and documentation standards, User training, Security, Back-up and storage guidelines, Password management, Personal usage policies, Software acquisition and usage standards, Data protection standards, Program maintenance and technical support, An appropriate level of segregation of duties and responsibilities, Virus protection, Encryption of key files, Installing a locking mechanism to control access to the on/off switch. This may not prevent PC theft, but may be effective in controlling unauthorized use, and implementing environmental controls to prevent damages from natural disasters, such as fire, floods, etc.'

C) The following techniques can limit access to programs and data to authorized personnel, using passwords, Implementing an access control package, Using of removable storage media, Using hidden directories and files, Using encryption.

D) Encryption is a technique that is generally used when sensitive data are transmitted over communication lines, but it can also be used on data stored on a stand-alone PC.

E) In a PC environment, users can generally perform two or more of the following functions in the accounting system:

i) Initiating source documents.
ii) Authorizing source documents.
iii) Entering data into the system.
iv) Processing data that have been entered.
v) Changing programs and data.
vi) Using or distributing output.
vii) Modifying the operating systems.\(^9\)

1002. IT Environments—On-line Computer Systems

As per online handbook issued by IFAC (2004) some vital points that had been mentioned under this above standard are:

A) On-line computer systems are computer systems that enable users to access data and programs directly through terminal devices. Such systems may comprise mainframe computers, minicomputers or a network of connected personal computers (PCs). When the entity uses an on-line computer system, the technology is likely to be complex and linked with the entity’s strategic business plans. The audit team may require special information technology (IT) skills to make inquiries and to understand the implications of the responses obtained.

B) On-line systems allow users to directly initiate various functions such as:

i) Entering transactions (for example, sales transactions in a retail store, cash withdrawals in a bank and shipment of goods in a plant)

ii) Making inquiries (for example, current customer account status or balance information)
iii) Requesting reports (for example, a list of inventory items with negative “on hand” quantities)
iv) Updating master-files (for example, setting up new customer accounts and changing general ledger codes)
v) Electronic commerce activities (for example, placing orders and paying for goods over the Internet).

C) On-line computer systems use many different types of terminal devices. Types of terminal devices are:
i) General Purpose Terminals, such as the following:
   * Basic keyboard and screen—used for entering data without any validation within the terminal and for displaying data from the computer system on the screen.
   * Intelligent terminal—used for the functions of the basic keyboard and screen with the additional functions of validating data within the terminal, maintaining transaction logs and performing other local processing.
   * PCs—used for all of the functions of an intelligent terminal with additional local processing and storage capabilities.
ii) Special Purpose Terminals, such as the following:
   * Point-of-sale devices—used to record sales transactions as they occur and to transmit them to the main computer.
   * Automated teller machines—used to initiate, validate, record, transmit and complete various banking transactions.
   * Hand-held wireless devices for entering data from remote locations.
   * Voice response systems—used to allow user interaction with the computer over a telecommunications network based on verbal instructions issued by the computer. The customer communicates using a tone-generating device, which is often the keypad on the customer’s telephone. Common applications include telephone banking and bill payment systems.
D) Employees, business partners, customers and other third parties may obtain access to an organization’s on-line applications by using the Internet or other remote access services. External parties may access the organization’s applications through electronic data interchange (EDI) or other electronic commerce applications.

E) Types of On-Line Computer Systems; On-line computer systems may be classified according to how information is entered into the system, how it is processed and when the results are available to the user. For purposes of this statement, on-line computer systems functions are classified as follows:

i) On-Line/Real-Time Processing

In an on-line/real-time processing system, individual transactions are entered at terminal devices, validated and used to update related computer files immediately. An example is the application of cash receipts directly to customers’ accounts. The results of such processing are then available immediately for inquiries or reports.

ii) On-Line/Batch Processing

In a system with on-line input and batch processing, individual transactions are entered at a terminal device, subjected to certain validation checks and added to a transaction file that contains other transactions entered during the period. Later, during a subsequent processing cycle, the transaction file may be validated further and then used to update the relevant master-file. For example, journal entries may be entered and validated on-line and kept on a transaction file, with the general ledger master-file being updated on a monthly basis. Inquiries of, or reports generated from, the master-file will not include transactions entered after the last master-file update.

iii) On-Line/Memo Update (and Subsequent Processing)

On-line input with memo update processing, also known as shadow update, combines on-line/real time processing and on-line/batch processing. Individual transactions immediately update a
memo file containing information that has been extracted from the most recent version of the master-file. Inquiries are made from this memo file. These same transactions are added to a transaction file for subsequent validation and updating of the master-file on a batch basis. For example, the withdrawal of cash through an automated teller machine is checked against the customer’s balance on the memo file, and is then immediately posted to the customer’s account on that file to reduce the balance by the amount of the withdrawal. From the user’s perspective, this system will seem no different from online/real time processing since the results of data entered are available immediately. However, the transactions have not been subjected to complete validation before the master-file update.

iv) On-Line/Inquiry

On-line inquiry restricts users at terminal devices to making inquiries of master-files. In such systems, the master-files are updated by other systems, usually on a batch basis. For example, the user may inquire of the credit status of a particular customer before accepting an order from that customer.

v) On-Line Downloading/Uploading Processing

On-line downloading refers to the transfer of data from a master-file to an intelligent terminal device for further processing by the user.

F) The characteristics of on-line computer systems may apply to many of the types of on-line systems discussed in the previous section. The most significant characteristics relate to on-line data entry and validation, on-line access to the system by users, possible lack of visible transaction trail and potential access to the system by non-users, including programmers and other third parties (for example, through e-mail and the Internet). The particular characteristics of a specific on-line system will depend on the design of that system.

G) When data are entered on-line, they are usually subject to immediate validation checks.
H) Applications in an on-line environment may have greater exposure to unauthorized access and update. An entity’s security infrastructure plays an important part in ensuring the integrity of the information produced. The auditor, therefore, considers the security infrastructure before examining the general and application controls.

I) These controls may include the use of passwords and specialized access control software, such as on-line monitors, that maintains control over the menus, authorization tables, passwords, files and programs that users are permitted to access. They may also include physical controls such as the use of key locks on terminal devices, locked computer rooms and inactivity timeouts. Other important aspects of control in an on-line computer system include: Controls over passwords, System development and maintenance controls, Programming controls, Transaction logs, Firewalls.\(^\text{10}\)

1003. IT Environments—Database Systems

As per online handbook issued by IFAC (2004) some vital points that had been mentioned under this above standard are:

A) A database is a collection of data that is shared and used by many different users for different purposes. Each user may not necessarily be aware of all the data stored in the database, or of the ways that the data may be used for multiple purposes. Generally, individual users are aware only of the data that they use and may view the data as computer files utilized by their applications.

B) When an entity uses a database system, the technology is likely to be complex and may be linked with the entity’s strategic business plans. The audit team may require special information technology (IT) skills to make appropriate inquiries and to understand the implications of the responses obtained. The auditor may need to use the Work of an Expert.

C) Database systems consist principally of two components: the database and the database management system (DBMS). Database systems interact with other hardware and software aspects of the overall computer system. 

D) The software that creates, maintains and operates the database is referred to as DBMS software. Together with the operating system, the DBMS facilitates the physical storage of the data, maintains the interrelationships between the data, and makes the data available to application programs. It also provides controlled access methods to establish basic security measures over the data. Usually, the DBMS software is supplied by a commercial vendor but will need to be adapted to the entity’s needs. 

E) Database systems are distinguished by two important characteristics: data sharing and data independence. These characteristics ordinarily require the use of a data dictionary and the establishment of a data resource management. 

F) Data Sharing; A database is composed of data set up with defined relationships and organized to permit many users to use the data in different application programs. 

G) Data Independence from Application Programs; The DBMS records the data once for use by various application programs. This creates a need for data sharing and a need for data independence from application programs. In non-database systems, separate data files are maintained for each application. Similar data used by several applications may be repeated in several different files. In a database system, however, a single file of data (or database) is used by many applications, with data redundancy kept to a minimum. 

H) Data Dictionary; A significant implication of data sharing and data independence is the potential for the recording of data only once for use in several applications. Because various application programs need to access these data, a software facility is required to keep track of the location of the data in the database. This software within the DBMS is known as a data dictionary. It also serves as a tool to
maintain standardized documentation and definitions of the database environment and application systems. A data dictionary provides functions such as: A facility to create or modify data definitions, Validation of the data definitions provided to ensure their integrity, Prevention of unauthorized access or manipulations of the data definitions, Interrogation and reporting facilities that allow the database administrator to make inquires on the data definitions.

I) Data Resource Management; Data resource management forms an essential organizational control in ensuring data integrity and compatibility. In a database environment the methods of informational control and usage change from an application orientated approach to an organization-wide approach. In contrast to traditional systems where each application is a separate system with its own reporting and controls, in a database environment, many controls may be centralized and the database is designed to serve the entire information needs of the organization.

J) Data Administration; The data administration function manages data as an organizational resource and includes responsibilities for: The development and implementation of a data resource management strategic plan and policies, The creation and maintenance of a corporate data model or architecture (sometimes referred to as an enterprise data model); The coordination and integration of system data models, Obtaining agreement among users about definitions and format of data, Resolving conflicts about incompatible representation and data, Establishing a corporate-wide data dictionary and managing the organization’s naming and definition standards, Establishing data standards and procedures for: data naming, data usage, data security, data definition compilation, data modelling, and Providing training and consulting to users and the data information technology team members (system developers and database administrators) concerning all aspects of data resource management.
K) Coordination is usually the responsibility of a group of individuals who are typically referred to as ‘database administration’. The individual who heads this function may be referred to as the database administrator. Generally, the database administration function takes responsibility for the definition, structure, security, operational control and efficiency of databases, including the definition of the rules for accessing and storing data.\(^{11}\)

**1008. Risk Assessments and Internal Control—CIS Characteristics and Considerations**

As per online handbook issued by IFAC (2004) some vital points that had been mentioned under this above standard are:

A) The use of computers may result in the design of systems that provide less visible evidence than those using manual procedures. In addition, these systems may be accessible by a larger number of persons. System characteristics that may result from the nature of CIS processing include the following:

i) Absence of input documents
ii) Lack of visible transaction trail
iii) Lack of visible output
iv) Ease of access to data and computer programs

B) The internal controls over computer processing, which help to achieve the overall objectives of internal control, include both manual procedures and procedures designed into computer programs. Such manual and computer control procedures comprise the overall controls affecting the CIS environment (General CIS controls) and the specific controls over the accounting applications (CIS Application controls).

C) The purpose of General CIS controls is to establish a framework of overall control over the CIS activities and to provide a reasonable

---

level of assurance that the overall objectives of internal control are achieved.
D) The purpose of CIS Application controls is to establish specific control procedures over the accounting applications in order to provide reasonable assurance that all transactions are authorized and recorded, and are processed completely, accurately and on a timely basis.\textsuperscript{12}

\textbf{1009. Computer-Assisted Audit Techniques (CAATs)}

As per online handbook issued by IFAC (2004) some vital points that had been mentioned under this above standard are:
A) The overall objectives and scope of an audit do not change when an audit is conducted in a computer information technology (IT) environment. The application of auditing procedures may, however, require the auditor to consider techniques known as Computer-Assisted Audit Techniques (CAATs) that use the computer as an audit tool.
B) CAATs may improve the effectiveness and efficiency of auditing procedures. They may also provide effective tests of control and substantive procedures where there are no input documents or a visible audit trail, or where population and sample sizes are very large.
C) CAATs may be used in performing various auditing procedures, including the following: Tests of details of transactions and balances, Analytical procedures, Tests of general controls, Sampling programs to extract data for audit testing, Tests of application controls, Reperforming calculations performed by the entity’s accounting systems.
D) CAATs may consist of package programs, purpose-written programs, utility programs or system management programs.

Regardless of the origin of the programs, the auditor substantiates their appropriateness and validity for audit purposes before using them.

i) Package programs are generalized computer programs designed to perform data processing functions, such as reading data, selecting and analysing information, performing calculations, creating data files and reporting in a format specified by the auditor.

ii) Purpose-written programs perform audit tasks in specific circumstances.

iii) Utility programs are used by an entity to perform common data processing functions, such as sorting, creating and printing files.

iv) System management programs are enhanced productivity tools that are typically part of a sophisticated operating systems environment, for example, data retrieval software or code comparison software. As with utility programs, these tools are not specifically designed for auditing use and their use requires additional care.

E) The auditor sometimes builds embedded audit routines into an entity’s computer system to provide data for later use. These include the following:

i) Snapshots: This technique involves taking a picture of a transaction as it flows through the computer systems. Audit software routines are embedded at different points in the processing logic to capture images of the transaction as it progresses through the various stages of the processing. Such a technique permits an auditor to track data and evaluates the computer processes applied to the data.

ii) System Control Audit Review File: This involves embedding audit software modules within an application system to provide continuous monitoring of the system’s information is collected into a special computer file that the auditor can examine.

F) Test data techniques are sometimes used during an audit by entering data (for example, a sample of transactions) into an entity’s computer system, and comparing the results obtained with predetermined results.
An auditor might use test data to:

i) Test specific controls in computer programs, such as on-line password and data access controls;

ii) Test transactions selected from previously processed transactions or created by the auditor to test specific processing characteristics of an entity’s information systems.\textsuperscript{13}

5.3. EDP AUDITING SYSTEM IN BANKS

In this section respectively, definition of bank and its characteristics, special auditing consideration in banks, the position of EDP system in banks, internal controls in EDP system (General and Application) in bank and EDP controls related to banking system through Internal Control Checklist would be as follows discussed:

5.3.1. Definition of bank and its characteristics

A bank is a kind of financial institution who’s principal and traditional activity is to collect funds (depositing or borrowing) from one group of people and to lend these collected funds (investment) to other group of people. In this cycle, one party who has funds but no idea and not able to work with this funds, other party who has idea to work with money but has no sufficient capital to set up this idea, other more party who has capital, reputed brand name, etc. and the last party who is as supervisory board as regulatory authorities in any countries are involved, so that this process is required to enter into a system that is known as banking system in where the operation and functions of this financial system can be performed into two kinds that is to be called Conventional banks and Islamic banks. Nowadays all banks through E-banking that is the product of EDP systems are struggling to cover and support new wants of their customers i.e. choice, convenience and control through modern banking services in

Analysis of EDP Auditing System in Banks

anywhere, anytime and anyway at minimum time and maximum quality in 24 hours banking service and 7 days banking work.

Characteristics of a bank that are caused to distinguish banking industry from other industry may be listed as follows:

i) Banks as custodians of the public money that directly are in public interests involved.

ii) Banks as intermediary role who facilitate mobilization of funds through collecting of deposits and allocating of these collected deposits to businessmen, entrepreneur and other group of people in the society.

iii) Because of significant role in all economic sections, control of operation in banks has been as the most practice watched.

iv) Because of progress and advancements in technology and communication, the operation of banks from manual tools must improve to computerization.

v) Computers are extensively used to process data and to generate Management Information now.

vi) Custodian of huge amounts of monetary items such cash and negotiable instruments.

vii) A loss of confidence by depositors in a bank’s solvency may quickly result in a liquidity crisis.

viii) Multiple and complicated accounting and internal control systems and widespread use of computer information system.

ix) Through E-banking products such as Internet banking, some transactions can be directly initiated and completed by the customer without any intervention by the bank’s employees.

5.3.2. Special auditing considerations in banks

As per online handbook issued by IFAC (2004), International Auditing Practice Statements (IAPSSs), Standard 1006 ‘Audits of the Financial Statements of Banks’ Paragraphs 73 to 79, audit procedures for obtaining audit evidence in bank that in manual system and computerised system are the same but tools and techniques are vary
through which by an auditor may be followed can be divided as under:

5.3.2.1. Inspection: It consists of examining records, documents, or tangible assets such as Securities, Loan agreements, Collateral, and Commitment agreements such as asset sales and repurchases, Guarantees. In an EDP system, depending on the level of computerization, evidence and documents are available on the form of database.

5.3.2.2. Observation: It consists of watching and looking the various stages of an output that as a result of an EDP system are processed and worked such as the stages of depositing.

5.3.2.3. Inquiry and confirmation: Inquiry consists of seeking information of knowledgeable persons inside or outside the entity. Confirmation consists of the response to an inquiry to corroborate information contained in the accounting records such as Collateral, Verifying or obtaining independent confirmation of, the value of assets and liabilities that are not traded or are traded only on over-the-counter markets, Asset, liability and forward purchase and sale positions with customers and counter-parties such as: Outstanding derivative transactions, Securities held by third parties, Loan accounts, Deposit accounts, Guarantees, and Letters of credit, Legal opinions on the validity of a bank’s claims.

5.3.2.4. Computation: This consists of checking the arithmetical accuracy of source documents and accounting records or of performing independent calculations. In the context of the audit of a bank’s financial statements, computation is a useful procedure for checking the consistent application of valuation models.

5.3.2.5. Analytical procedures: They consist of the analysis of significant ratios and trends including the resulting investigation of fluctuations and relationships that are inconsistent with other relevant information or deviate from predicted amounts.14

As per online handbook issued by IFAC (2004), International Auditing Practice Statements (IAPSs), **Standard 1006 ‘Audits of the Financial Statements of Banks’** Paragraphs 21 and 45 the **risks** associated with banking activities and audit risk may broadly be categorized as:

5.3.2.6. **Country risk**: The risk of foreign customers and counter parties failing to settle their obligations because of economic, political and social factors of the counter party’s home country and external to the customer or counter party;

5.3.2.7. **Credit risk**: The risk that a customer or counter party will not settle an obligation for full value, either when particularly from commercial lending, may be considered the most important risk in banking operations.

5.3.2.8. **Currency risk**: The risk of loss arising from future movements in the exchange rates applicable to foreign currency assets, liabilities, rights and obligations.

5.3.2.9. **Fiduciary risk**: The risk of loss arising from factors such as failure to maintain safe custody or negligence in the management of assets on behalf of other parties.

5.3.2.10. **Interest rate risk**: The risk that a movement in interest rates would have an adverse effect on the value of assets and liabilities or would affect interest cash flows.

5.3.2.11. **Legal and documentary risk**: The risk that contracts are documented incorrectly or are not legally enforceable in the relevant jurisdiction in which the contracts are to be enforced or where the counter parties operate.

5.3.2.12. **Liquidity risk**: The risk of loss arising from the changes in the bank’s ability to sell or dispose of an asset.

5.3.2.13. **Modelling risk**: The risk associated with the imperfections and subjectivity of valuation models used to determine the values of assets or liabilities.
5.3.2.14. Operational risk: The risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events.

5.3.2.15. Price risk: The risk of loss arising from adverse changes in market prices, including interest rates, foreign exchange rates, equity and commodity prices and from movements in the market prices of investments.

5.3.2.16. Regulatory risk: The risk of loss arising from failure to comply with regulatory or legal requirements in the relevant jurisdiction in which the bank operates.

5.3.2.17. Reputational risk: The risk of losing business because of negative public opinion and consequential damage to the bank’s reputation arising from failure to properly manage some of the above risks, or from involvement in improper or illegal activities by the bank or its senior management, such as money laundering or attempts to cover up losses.

5.3.2.18. Settlement risk: The risk that one side of a transaction will be settled without value being received from the customer or counter party. This will generally result in the loss to the bank of the full principal amount.

5.3.2.19. Solvency risk: The risk of loss arising from the possibility of the bank not having sufficient funds to meet its obligations, or from the bank’s inability to access capital markets to raise required funds.

5.3.2.20. Transfer risk: The risk of loss arising when a counter party’s obligation is not denominated in the counter party’s home currency.

And finally, three components of audit risk are:
A) Inherent risk (the risk that material misstatements occur);
B) Control risk (the risk that the bank’s system of internal control does not prevent or detect and correct such misstatements on a timely basis); and
C) Detection risks (the risk that the auditor will not detect any remaining material misstatements).\(^{15}\)

Therefore the EDP system change the environment in where the banks execute their functions and accordingly the auditors are involved with new risks to manage securities of new banking products upon that derived from the E-banking such as the security and privacy of transmissions throughout the Internet and the completion, accuracy, timeliness and authorization of Internet transactions as they are recorded in the bank’s accounting system.

5.3.3. The Position of EDP system in Banks

Today the banking system, whether Islamic or conventional plays a vital role in all economic sections and Information Technology (IT) creates an environment in that, enables the banks:

5.3.3.1 To handle efficiently much larger capacity and volumes of business:

i) Supply and support banking services on the basis of real time

ii) Maximize the profitability

iii) The claim to be anywhere, anytime and anyway

iv) Reduce the cost of products

v) Catching the customers in local as well as international areas so that the ultimate banking targets that is bringing merchant, commercial and investment-banking functions under an umbrella service or universal banking could be achieved.

The Islamic banking system as a young phenomenon in the baking industry has the serious thinkable issues in where its growth in the world is reasonable and promising. The Islamic banks are much more functioning in developing as well as less developed countries in where these countries are characterized with:

i) Lack of required telecommunication infrastructure

Chapter Five

ii) Inadequate focus in international language
iii) Unsure of security of transactions
iv) Inadequate investment in hardware and software

Therefore the level of EDP system depends on the banks in where laid down and generally in developed countries the products of modern banking such as Internet banking are with high quality presented and in the developing as well as less developed countries may the products of E-banking are not as the same quality in developed countries presented. Therefore it can be stated that the extend of EDP system in banks are:
i) To present the new products of E-banking, the IT in banks is as a must.
ii) To process a large volume of transactions, the EDP system is as a compulsory think for banks.
iii) To calculate arithmetic activities (interest or profits, etc.) whether in payment or received form, for a large volume of borrowing and lending.

And to sum up this section it would be valuable to express that the use of IT and telecommunications systems are widespread using in banks and audit of such system has the most significant issues in the new millennium.

5.3.4. Internal controls in EDP system in bank

Internal controls in banking industry have significant and vital impacts on such business, so an effective system of internal controls is a basic component of bank management and a foundation for the safe and sound operation and can help to ensure that the goals and objectives of a banking organisation would be in efficient and efficient way achieved. So understanding of these controls for auditors sufficient to identify and appraisal the risks associated to such business whether due to fraud or error, and sufficient to design and perform further audit procedures have been as a necessity considered. In where a bank utilizes the electronics to initiate, record,
process, and report transactions, records in electronic format replace with paper documents so audit trail may be in difficulty traced. Controls in IT systems consist of a combination of automated controls and manual controls depending the nature and complexity of the use of EDP in the bank.

According to The Basle Committee on Banking Supervision (1988) that introduced the framework for internal control, significant considerations about internal control systems in banking organizations can be stated as follows:

As per Paragraph 4, page 8 of this framework, the main objectives of internal control are:

i) Efficiency and effectiveness of activities (performance objectives)

ii) Reliability, completeness and timeliness of financial and management information (information objectives)

iii) Compliance with applicable laws and regulations (compliance objectives)

As per principle 7, 8 and 9 about Information and communication of this framework:

A) An effective internal control system requires that there are adequate and comprehensive internal financial, operational and compliance data, as well as external market information about events and conditions that are relevant to decision making. Information should be reliable, timely, accessible, and provided in a consistent format.

B) An effective internal control system requires that there are reliable information systems in place that cover all significant activities of the bank. These systems, including those that hold and use data in an electronic form, must be secure, monitored independently and supported by adequate contingency arrangements.

C) An effective internal control system requires effective channels of communication to ensure that all staff fully understand and adhere to policies and procedures affecting their duties and responsibilities and that other relevant information is reaching the appropriate personnel.
As per pages 6 and 7, the types of control breakdowns typically seen in problem bank cases can be grouped into five categories:

i) Lack of adequate management oversight and accountability, and failure to develop a strong control culture within the bank

ii) Inadequate recognition and assessment of the risk of certain banking activities, whether on- or off-balance sheet

iii) The absence or failure of key control structures and activities, such as segregation of duties, approvals, verifications, reconciliation, and reviews of operating performance

iv) Inadequate communication of information between levels of management within the bank, especially in the upward communication of problems

v) Inadequate or ineffective audit programs and monitoring activities.  

5.3.5. EDP Controls in bank through Internal Control Checklist

As mentioned earlier a bank is a financial institution upon which the main its practice is borrowing and lending money as an intermediary role to get interest or profit. Today because of progress and advancement in technology, the banks through E-banking or new concept of modern banking that is the product of Information technology, have some new products such as Internet banking introduced to support the fresh wants of their customers. This trend from one hand has facilitated the services of modern banking and from other hand, scrutiny of all level of bank’s management assesses

---

16 Researcher’s Note: The Basle Committee on Banking Supervision is a Committee of banking supervisory authorities, which was established by the central bank Governors of the Group of ten countries in 1975. It consists of senior representatives of bank supervisory authorities and central banks from Belgium, Canada, France, Germany, Italy, Japan, Luxembourg, Netherlands, Sweden, Switzerland, United Kingdom and the United States. It usually meets at the Bank for International Settlements in Basle, where its permanent Secretariat is located. FRAMEWORK FOR INTERNAL CONTROL SYSTEMS IN BANKING ORGANISATIONS Basle Committee on Banking Supervision, Basle, September 1998 For more details and information refer to: www.bis.org and also www.bis.org/publ/bcbs40.htm (Visited on 10,01,2006)
and appraisal of this trend has been essentially required. In other words the management have got to create new products upon which they are based on IT and paperless documentation and also they have got to create necessary ways and approaches to assess and control such new products so that the predetermined goals and objectives in effectiveness (doing right things), efficiency (doing them well) and economy (doing them economic) performing achieved. Therefore the performance of EDP system must be controlled and audited, means EDP systems must be assessed and audited to scrutiny that the computer system safeguard assets, maintain data integrity, and achieve the predetermined goals and objectives of bank effectively and efficiently and economic.

Accordingly EDP activities in bank in both departments and branches are generally to be brought under the assessment and appraisal of Inspection and Audit department to ensure that computerized activities in departments and branches are under an effective, efficient and economic controls according to computerised environment so goals and objectives of bank effectively and efficiently and economically achieved.

So a bank should have proper and appropriate controls to manage its risks, accurate measurement and reporting of positions, verification and approval of transactions, reconciliation of positions and results, setting of limits, reporting and approval of exceptions to limits, physical security and contingency planning relating to EDP activities and for this purpose in the following paragraphs areas of risk in the computerised environment in bank are to be neither definitive nor comprehensive, but rather to provide some general as to the nature of controls that could be found in practice as under through checklists or questionnaire presented:

Therefore the auditor must see special considerations during the bank audit and the management of bank must provide such requirements to improve the bank operation and accessibility of bank objectives that through bank strategy have been documented.
Accordingly to continue these considerations the following discussions related to banking system are to be stated:

5.3.5.1. Fundamentals in EDP system
5.3.5.2. Human resources in EDP system
5.3.5.3. Management responsibilities in EDP system
5.3.5.4. Controls in EDP system

5.3.5.1. Fundamentals in EDP system

According to Kell and Boynton (1992):

A) **EDP System** can be defined as the methods and techniques associated with the organising and processing of data by an electronic machine i.e. a computer or the act of such process called Computer Information System, Computing, Information Processing, Information Systems, Management Information System, etc.

B) **EDP Assets** consist of Computers Hardware and associated peripherals computer, Computer rooms including EDP department, Users departments and branches and other off-site storage areas, telecommunications networks and facilities.

C) **EDP information assets (also called EDP information)** comprise of computer systems software, applications systems software, programs, files, database, and copies thereof on paper or other media.

D) **Documentation** of such procedures, systems, application systems designs, change management, contingency and disaster recovery plans as are required to assure the continued run of bank business.

E) Basic Component of EDP System:

i) **Computer Hardware consists of** physical equipment associated with the systems such as central processing unit (CPU), input and output devices.

ii) **Computer Software** consists of programs and routines that facilitate the programming and operation of a computer and are two types:

a) System Programs to conduct specific tasks and include:
* Operating system; Operation of computer including inputs, outputs, main storage, execution of programs and management of files, etc. are directed through.

* Utility programs; Common data processing tasks like printing, recognising data in files, copying, etc. are performed through.

* Compilers and assemblers; A specific programming language is translated into understandable language through a computer.

* Database management system; the data records and files separately of the application programs that allow changes in or use of data are controlled through.

b) Application Programs consist of instructions that the computer is enabled to process a bit of specific tasks for the user. Examples are Excel or Tally for accounting and Access for database, etc.

iii) Data organization methods;
This term refers to the way that data are organized within a computer file, the two principle methods of data organization are:

a) Traditional file method consists of two kinds;
   * Master files that consist up-to-date information about a given class of data such as current or savings balances of customers’ accounts.
   * Transaction files that consist the details of individual transactions of the same class such as credit or debit over current account of a specific period like a day. Under this method, separate master and transaction files for each application such as current accounts or savings accounts are maintained.

b) Database method; This method is based on the creation and maintenance of a single common direct access file for all application using common data so that each data element is stored only once, but it is accessible by all authorised application programs.

iv) Data processing methods;
This term refers to the way that data are entered into and processed by the computer. There three method that are widely used.
a) Batch Entry/ Batch Processing; Data are accumulated by classes of transactions such as current accounts or saving accounts and both entered and processed in batches.
b) On-line entry/ batch Processing; Individual transactions are entered directly into a computer via a terminal as they occur but data are subjected to specific edit or validation checks by computer program at the time of entry and error message are communicated promptly to the terminal operator. A machine-readable validated transaction file is accumulated as the transactions are entered. This file is subsequently processed to update the master file.
c) On-line entry/ On-line processing; Under this method the master files are update concurrently with data entry, and a transaction log is produced that consist of a chronological record of all transactions that each transaction is assigned a unique identifying number by computer program. Generally to cover the risk of errors in master files from concurrent updating and the possible loss of part or all the master files in case of hardware failure, memo updating of the master file at the time of data entry involving a copy of master file is used.17

5.3.5.2. Human resources in EDP system

Human Resources in EDP environment plays a significant role so that, its function is required to gain particular skill and knowledge and also must be accompanied with progress and advancements of technology. Bank Administration Institute, (1968)18 believe that “EDP personnel generally do not access to cash... the lack of access to cash can be circumvented by EDP personnel through improper credits to their own accounts or by the diversion of their debits to other accounts”. Therefore in the following the organisational structure of

18 BAI, Bank Administration Institute, "Auditing bank EDP Systems Prepared By Audit Commission", Park Ridge BAP, 1968, P. 86
EDP department in common view relevant to bank through clear-cut lines of responsibilities and authority that is to be shown in exhibit 5.1 are to be presented:

A) **EDP management**: Head of EDP department through his Vice-president, has overall responsibility for the planning, developing and controlling all computer information system and also responsibility to provide short as well as long term plans related to EDP system and additionally it must provide necessary information as inputs for top management to provide their decision-making function.

B) **Systems Analyst**: Has responsibility to appraisal existing system, design and develop new system and prepare specification for programmer.

C) **Programmers**: Have function and responsibility for programming new systems including flowcharts, develops, documents and debugs the programs, and maintaining exiting programmes.

D) **Database administrators**: Have responsibility to design, use and control data dictionary or database and library of application system files.

**Exhibit 5.1**: Organisational chart of EDP department in a bank
E) **Data security administrators**: Have responsibility of the physical security of data processing installation including input, processing and output and also negotiation with users departments to improve the stage of data processing.

F) **Operators**: Have responsibility of daily operation of data processing including data preparation, control over production applications and files, hardware and totally the daily operation of EDP system would be left by them.

G) **Librarian**: Responsibility of custody of data and programmes and systems documentation.

5.3.5.3. Management responsibilities in EDP system

Management (Board of Directors) is responsible for the overall corporate governance of the bank. Its principal role is to formulate and place strategies, establish policy guidelines and ensure that the bank is running in an efficient and effective manner. Management is responsible to understand issues and problems related to EDP system and they must be considered in planning, organizing, staffing, directing and controlling as five principles management functions. Therefore management have got to ensure that:

A) The business objectives, Long-term plans as well as short-term plans, assets safeguarding, system effectiveness and system efficiency, sound system of internal controls are to be through EDP systems facilitated.

B) To cover these above issues, justification of establishment of EDP system instead and in parallel use of manual and mechanical systems in safety and secure environment has got to be provided.

C) Required skilled human resources to set up and run EDP systems could be achieved so that the internal competition as well as external competition would be in willing and promising manner facilitated.

D) Required infrastructure facilities and necessary equipments in which environment that the bank in running its function is with
reasonable acceptance to be covered through state so willing and satisfaction of customers could be achieved.

Therefore internal controls checklist for business strategy related to EDP system that may be followed by auditors and inspectors of bank could be listed as follows:

a) Has the role of EDP system in documented business strategy clearly defined?

b) Has the relationship between the bank objectives and EDP system in documented business strategy adequately and clearly described?

c) How does management ensure to get necessary information concerning to effectiveness and efficiency of EDP system activities?

d) Is there any terms and provisions in documented strategy to ensure that the requirements of EDP systems including hardware, software, organisations and processing of data are developed and acquired under the authorisation of board of director?

e) Whether reasonable and acceptable measures of acquisition and development of EDP systems components through Board of director in documented strategy have been provided?

f) Whether adequate financial resources are allocated to EDP system components?

g) Is there any reasonable indexes to measure the economy of EDP system activities in compare to allocated financial resources?

h) Has management adequately described the organisational structure of EDP department?

k) Has management adequately described the administrative controls in EDP department?

l) Has management adequately described necessary terms and provisions for the environmental controls for EDP department?

5.3.5.4. Controls in EDP system

Generally controls in EDP system related to banks can be classified into two major categories namely General controls and Application controls. The exhibit 5.2 is useful summary of this classification as shown under:
A) General Controls

These controls are over the entire EDP environment in where the activities of EDP system through a computer are executed. These controls are involved to review the organisational structure of EDP systems, system development, physical security of both hardware and software, access to EDP equipments and also data and information and documentation so to ensure that applications in EDP environment can adequately and smoothly run.

Exhibit 5.2: Controls, related to EDP system in a bank

a) Organisational Controls
Definition:

Organisational controls are those provided to review of internal controls related to organisational structure of EDP department so that segregation of duties between EDP department and user departments and also within various sections of EDP department are focused. The clear-cut lines of responsibilities in organisational structure have to assure development, implementation, operation and maintenance of computer information system in a planned and controlled manner so that segregation of duties as an important internal control in bank are to be facilitated. These controls are those related to the method of assigning authority and documentation of EDP systems including design; develop of programs and maintenance of such programs with respect to available standards, insurance coverage and statement concerning the plans and budget. Weakness in such controls affect entirely the EDP applications and strength in them will cause the efficient organisational structure, accountability and responsibility, adequate skilled human resources, appropriate of standards, proper segregation of duties and so on in EDP department.

Checklist:
* Determine if the board has properly defined the organisational structure of EDP department?
* Determine if the Head of EDP department report to the board.
* Determine if the organisational structure is reviewed and necessary adjustment according to progress of EDP system due to technological advancements are to be in place taken.
* Determine if EDP department is organisationally independent from user department.
* Determine if data is formally transferred between EDP departments from user department.
* Determine if duties such as authorisation, initiation of transactions is performed out of EDP department.
* Determine if source of documents and correction of errors occurred in them is provided out of EDP department.
* Determine if personnel policy in EDP department is formulised and documented.
* Is there adequate organisational chart in EDP department to show proper clear-cut lines of authority?
* Is there adequate job description for each job in EDP department?
* Determine if segregation of duties among various positions in EDP department provide sufficient and adequate caution to prevent their responsibilities of such positions to each other.
* Determine if segregation of duties provide and assign adequate separation among each section of EDP department so every position are forbidden to operate and run other position.
* Are there any written statements to employ the new staff as per required skills?
* Determine if necessary standards for the following EDP activities have been authorised and documented and on such basis are to be implemented.
  i) EDP section in all branches of bank
  ii) EDP section of all departments other than EDP department
  iii) All short as well as long term EDP plans
  iv) Data back-up and media handling procedures
  v) Adequate and sufficient insurance coverage for internal fraudulent and embezzlement activities
  vi) Any adequate insurance plan to cover external fraudulent and embezzlement activities like attacks of Hacker to A/C of customers
  vii) Budget for short as well as long term EDP projects or plans
  viii) As an comparison view actual budget vs. estimated budget
  ix) Changes in all kind of EDP systems and programmes

b) Physical Environmental Controls
Definition:
Environmental Controls are those concerned to terms and provisions of an adequate and safe EDP environment. Under these controls it could be assured that the EDP installations are in an adequate and reliable environment against unwanted and unexpected hazardous events such as fire, flood, etc. and otherwise corrective adjustments.

Checklist:
* Determine if necessary facilities in during construction or development of EDP premises have been considered in place to protect EDP installation from power, fuel, water, heating, cooling, etc.
* Determine if EDP components have situated in a building in where fire resistant and wall, floor and false ceiling are non-combustible.
* Are there adequate power sources to support operations and performance of EDP installation and also have been in place necessary alternative and helping power sources such as uninterruptible power supply or Emergency Power System e.g. generators for unexpected times placed?
* Determine if emergency power-off procedures are laid down and evacuation plan with clear responsibilities in place.
* Determine if fire detection and alarm system such as fire suppression equipment e.g. dry line water suppression and extinguishers or ozone friendly gas smothering system for computer room are in existence.
* Determine if fire prevention and control measures implemented are adequate and tested regularly.
* Determine if fire instructions are clearly posted and fire alarm buttons clearly visible
* Determine if smoking restriction in computing facilities are in place.
* Determine if smoke/heat-rise detectors installed and connected to the fire alarm system.
* Determine if fire drill and training are conducted periodically?
* Determine if EDP components are located above ground level, then determine if water leakage, seepage etc. are prevented.
* Determine if air-conditioning, ventilation and humidity control procedures are in place, tested periodically and given adequate attention.
* Determine if alternative water, gas, air-conditioning and humidity resources are available.
* Determine if adequate controls are in place to prevent and protect the EDP installation from water leakage and if water is used to cool EDP installation, related means must be checked.
* Determine if adequate controls concerning to emergency lighting, shutdown procedure are in place.

c) Physical Security and Access Controls

Definition:
These controls are those designed to prevent unauthorized use of EDP components including hardware and software such as all physical equipments, files, programmes and documents and communication facilities. Therefore computer equipments must be protected from hazardous events like fire and data and programmes must be protected from loss and unauthorized use and unauthorized change. Accordingly under these controls it could be assured that the EDP installations are in an adequate and reliable environment so only authorized personnel can access to EDP premises and installation.

Checklist:
* Determine if a well-based physical security and access policy has been documented.
* Is the policy specially to accompany with technological progress regularly revised?
* Determine if the policy take into account the following areas in EDP department, user departments and branches;
  i) Legal as well as regulatory requirements
  ii) Physical security to computer installations
  iii) Physical security to location of EDP components
iv) Physical security to access to EDP components
* Determine if the following major security areas are by policy covered:
  i) Physical Security to IS establishments
  ii) Handling of confidential information
  iii) Handling of security incidents
  iv) Privacy related issues for outside entities
  v) E-mail security
  vi) Application security
  vii) Interface Security
  viii) Password Security
  ix) Operating system security, web site security
  x) Database security
  xi) Anti virus and piracy policy
  xii) Archived and backed up data security
  xiii) Procedures for handling incidence of security breach
  xiv) Disaster recovery plan
  xv) Use of cryptology and related security
  xvi) Persons responsible for implementing security policy and consequence for wilful violation of the security policy
* Determine if access to computer room and telecommunications room and computer facilities restricted to only authorized personnel.
  i) Security guards for entering and leaving
  ii) Electronic locks and card-key system
  iii) Special keys
  iv) Double-entry doors
  v) Alarms on windows and doors
  vi) Sign-in and sign-out logs for all visitors (signage)
  vii) Surveillance cameras
  viii) Escort
  ix) Registration
Chapter Five

* Determine if EDP facility located in a place in which is not externally obvious.
* Determine if the physical access control procedures are adequate for employees, vendors, equipment and facility maintenance staff.
* Determine if periodic review of access profiles is carried out.
* Determine if revocation, response and escalation process in the event of security breach appropriate.
* Determine if security for portable and off-site devices adequate.
* Determine if all access routes are identified and controls are in place.
* Determine if the computer room is locked and access is restricted.
* Determine if hazardous commodities are not stored in the EDP area.
* Determine if data files and programmes are restricted to unauthorized access and use.
* Determine if physical controls exist in the form of a library and through librarian.
* Whether appropriate access controls like password, swipe card, biometric devices etc. are in place and adequate controls exist for storing the data / information on them?
* Wherever access to the EDP facility is enabled through ID cards / badges, etc., are there controls to ensure that the issue and re-collection of such access devices are authorized and recorded.
* In case of outsourced software, whether all maintenance work is carried out only in the presence of / with the knowledge of appropriate bank staff.
* Based on criticality of the IS facility, are there video surveillance equipments to monitor the movements of the personnel inside the facility? If so, check whether continuity of video recording is ensured.
* Whether access violations are recorded, escalated to higher authorities and appropriate action taken.
* Determine if access to communication equipment is restricted to computer operation staff and staffs of the telephone company who have need to access this equipment.

d) Security of Data Controls
Definition:
Through data security controls, the EDP operations are controlled to minimize the errors while processing data and also to support and backup EDP operation in during physical disaster and computer failure. The ability to reconstruct data files is the use of Grandfather, Father, Son (GFS) system or file dumping.

In GFS system a master file after a run towards updating will change to a new master file including previous data plus data through updating has been add to it. Exhibit 5.3 shows this process. Master file or grandfather e.g. current account ledger file is exist while new transactions e.g. debit or credit events occur so in this cycle this available master file must go to updating and while this run, the updating master file called as father or master file in updating run and after updating that is the adding of new transactions to grandfather (add debit or credit amount to previous balance into master file in updating run) and so new updated master file is called son.

Exhibit 5.3: A cycle of GFS system

Significant point of this system is that the master file or grandfather would be retained until the son comes into existence and so this cycle would be continued. In the event that the current computer master
A file is destroyed the system than has the capability to replace it. Ideally these three generations must be stored in separate location to minimize the risk of losing all files at one time. Exhibit 5.4 shows this process. Similar to this above approach is the file dumping in where the copy of a file or files after or before processing the data is provided and if a file in the processing time damaged or destroyed, the process can be started again through the copy of file.

Checklist:
* Determine if the off-premises storage or backup facilities for files, programmes and documentation is used.
* Determine if programmes and files through keeping in a library by a librarian is controlled.

Exhibit 5.4: An example of GFS system

* Determine if programmes files, standing data file, transaction data files, master files are labelled internally and externally.
* Determine if in GFS system till last generation of files through magnetic disks continuity of operations are assured.
* Determine if files in hard disk are frequently and regularly dumped.
* Determine if access to data through no access, read only, read and add, read and delete has been graded?
* Determine if the access to data through password is restricted.
* Determine if the password periodically is changed.
* Determine if proper controls to prevent and detect unauthorised access to data are in force.
* Determine if a tape management system (TMS) has been installed on the processing system that provides an inventory of tapes by location. Observe that the tapes that are maintained offsite have been properly segregated on the TMS.

B) System Acquisition Controls
Definition:
System Acquisition Controls and System Development Controls are related to initially survey and feasibility study, system design, programmes specifications, change to programmes, documentation procedure, implementation of system and as a feed back to such processes they must be tested, reviewed and modified and to implement these process the involvement and co-operative of a group including EDP department, user department, auditor and inspector department of bank are required. Review over System Acquisition and System Development in many controls is similar and in a few controls may vary. Generally System Acquisition relates to purchase of a new system to satisfy a service and System Development relates to develop an existing system to improve the quality of service that may include the acquiring the new system or change the existing the system. Therefore these kinds of reviews can be done separately or jointly. Accordingly in this research work for the purpose of more discussions, first System Acquisition and second System Development would be expressed.
Checklist:

a) *Initiation Phase*
* Determine if there is a plan that explains the need for new system.
* Is this plan according the bank overall EDP strategy?
* Determine if request for system acquisition is according to the definition of problem in which must be through new system supported.
* Determine if the plan approved and documented by the user and EDP departments.
* Determine if the finance of system has been budgeted as per overall EDP budget of the bank?
* Has the need for the system been defined with regards to the following details?
  i) User requirements
  ii) Technical requirements
  iii) Functionality and performance requirements
  iv) Security requirements
  v) Audit requirements
  vi) Documentation requirements

b) *Vendor Search*
* Determine if the search for vendor has in adequate and appropriate ways been done?
* How has the final selection of vendor been done?
* Identify those vendors who were included in the detailed review and analysis process, and indicate how and why the others were eliminated.

c) *Acquisition Phase*
* Do the EDP department have a technology standard such as Architecture, Open Database standards, Security Standards, etc. for product selection?
* Determine if the system selection approach consistent with the EDP platform of the bank.
* Does the bank have clearly laid down and approved guideline for selection of product vendors.
* Does the Vendor Selection guideline address the following?
  i) Market Presence
  ii) Years in operation
  iii) Technology alliances
  iv) Desired size
  v) Customer base and existing implementation
  vi) Support
  vii) Possibilities of partnership or strategic alliance
  viii) Source code availability
 ix) Local Support in case of foreign vendors
* Does the EDP department use scoring model for evaluating the products and vendor?
* Do the scoring criteria consider the following factors?
* Does the bank have a system of floating formal RFP (Request for Proposal) for systems with estimated budget exceeding a certain amount?
* Is there a core team comprising of personnel from EDP department, Functional departments and Internal Audit or Inspector department in charge of vendor selection and implementation?
* Are Meetings of the core team documented?
* Is final evaluation and selection fully documented and approved?
* Does the document clearly reflect the rationale used for the selection?
* Determine if there are appropriate terms and conditions established by Law department of bank to enter into a contract with the software vendor.
* Does the bank have approved terms and conditions for Product Licensing Agreements?
* Do the licensing terms contain?
  i) Escrow mechanism for source codes
  ii) Facilities for minor customisation
iii) Maintenance and upgrades
* Where the contract is entered with a distributor or reseller, is there a commitment to ensure that the actual owner would support the bank in case of relationship between the owner and the reseller breaks?
* Does the contract clearly segregate duties and responsibilities of the bank and the vendor?
* Does the contract include a clause to protect the bank from the vendor using the bank data?
* Does the contract clearly specify the product base lines?

d) Implementation Phase
* Is gap analysis between the requirement and the selected product carried out and documented?
* Does this document act as the basis for further implementation plans?
* Does the Bank’s policy provide for parallel run of previous system during the implementation period?
* Is there an agreed plan for implementation? Has the plan been approved by vendor and EDP Department?
* Does the implementation plan clearly identify product customisation requirements, user acceptance criteria and test for such customisation?
* Does the implementation plan address data migration from previous systems?
* Determine if the implementation cover the following:
i) User departments’ involvement and their role
ii) User training
iii) System administration training
iv) Acceptance testing
v) Role of vendor and period of support
vi) Required EDP infrastructure plan
vii) Risk involved and actions required mitigating risks
* Is there any practical analysis between the results achieved by new system against estimated results expected from such system?
* Is there any feedback of implementation of acquired system?
* Does Bank has a test environment to simultaneously allow familiarisation during the implementation process? Have errors identified during the implementation phase been documented and the root cause of the errors analysed and confirmed by the software vendor?
* Determine if test outputs is to be done and required analysis on final outputs with estimated outputs is to be done?
* Determine if there are any errors in the implementation phase and if so, has it been rooted through vendor.
* Is the result of testing properly documented?
* Are all following documents handed over by the vendor?
  i) System documentation (design and program documentation)
  ii) Data Dictionary
  iii) Installation Manual
  iv) User Manual
  v) Trouble Shooting
* Does the IT department have a proper archival system for these documents?
* In cases where source code is given by the vendor, has the IT department done a technical conversion and issued a confirmation of satisfactory compilation / performance?
* Has the IT department in consultation with User Department worked out database controls?
* Has IT department introduced a system to track problems reported by users, escalation to vendor and their resolution?
* Is there a system of measuring vendors’ support with the agreed service levels?
* Is there an identified System Administrator who is responsible for managing access to the system, back up and ensuring data base controls?
C) System Development Controls

Definition:

System Development Controls are related to initially survey and feasibility study, system design, programmes specifications, change to programmes, documentation procedure, implementation of system through its development and as a feed back to these process testing, review and modify of these phases through the involvement and cooperative of a group including EDP department, user department, auditor and inspector department of bank.

Checklist:
* Determine if a request was prepared regarding to a need of development of new or modify of a system prior to initiation of the development.
* Determine if such request have been through EDP and user departments approved and documented.
* Determine if such above request have been through board approved and documented and it is identified that the problem (request) must be supported by system development according to bank objectives.
* Determine if initially survey and feasibility study system development by qualified personnel have been conducted.
* This initially survey and feasibility should cover the following requirements;
  i) Problem definition
  ii) Need for system development including new, modify, etc.
  iii) Estimate the required budget
  iv) Estimate the required time
  v) Estimate the initiation date
  vi) Benefits of system development including new, modify, etc.
  vii) Benefits of system development as compared to old system
  viii) Consultation with user department of bank
ix) Consultation with Internal and Inspector department of bank
x) Consultation with external auditors where it is appropriate

* Determine if the following procedure in development of system have been considered;
  i) System design
  ii) Programming
  iii) Testing
  iv) File conversion

* Determine if does system design including the following;
  i) Descriptions and flowcharts
  ii) Kind of inputs
  iii) Kind of outputs
  iv) Programme files
  v) Standing data files
  vi) Master files
  vii) Explanation of inputs controls
  viii) Explanation of outputs controls
  ix) Equipments need
  x) Major risk
  xi) Standards
  xii) Processing routines
  xiii) Security matters

* There must be involvement in system development among EDP department, user department, Internal / Inspector department and in where it is appropriate accounting department.

* Have been the following considered in the setting of specifications of programmes?
  i) Formally set up standards
  ii) Specifications of inputs
  iii) Details of data in the each file, programme
  iv) Logic and approach of programming
  v) Documentation standards
  vi) Controls matters and management trails
vii) Testing of standards
viii) Operator instructions
* Have been the reports through user department approved?
* Have been specifications of programmes through user department approved?
* Is there any plan to test the system development?
* Is to be the results of test plan documented?
* Is to be the entire plan through EDP system analyst and users tested?
* Is to be the results of system development with the outputs of the old system compared?
* Is to be the results of this comparison documented?
* Determine if all involvements parties in system development have given their acceptance and consent by written satisfaction.
* Determine if the conversion of files has adequately on the basis of writing standards conducted and reconciled with original files.
* Review the training of operators and user staff to practice new system.

System software and Application software Controls
Ritchie (2005) says, combination of computer hardware, the means of processing and storage information and the computer software (programmes and applications) the means of doing tasks provide us a total useable system. Software can be classified into two groups i.e. system software and application software. Application software consists of the programmes which carry out the specific processing required for user applications e.g. accounting system but System software is not application specific, it is oriented to the needs of the hardware and facilitates the development and running of applications and the most significant item of system software is the operating system. Operating System is primarily a provider and manager of machine resources; the physical resources of a computer are the processor, main memory, secondary storage, input /output
devices. Access to these resources is centralised and controlled by various modules of the system. In addition to this role, the operating system provides other services such as user interface, data security, etc. In other words the most end users of enterprise systems rarely interact with the operating system, they interact with the applications for instance the customer of a bank logs in directly to a screen that prompts for inputs required for withdrawal of monies or other transactions. Application software such as retail banking, financial accounting and invoicing are what users log into depending on their roles in the organization. Application software sits on top of the operating system (with a database management system, also on top of the OS). A user does not need to know what OS is being used, and the user’s only interaction is with the application software.  

Accordingly EDP auditor needs to be concerned about the operating system for the following reasons. The operating system sees all data on the disk as streams of bits in the records inside the files and folders. The operating system does not see the data relating to the basic pay of an employee as being significantly more or less sensitive than the employee's telephone number. It is the application software that understands the data from the business perspective; all business rules relating to the way the data can be manipulated are enforced through programs in the application software. For example, the application software does not allow a banking customer to modify the balance in the account, but only displays it and accepts a transaction. Good application software has controls designed to enforce all the validations and business rules relating to who interacts with which elements of the data and how. As long as the user stays within such an application, the user's actions are well controlled. Most application users log directly onto an application and, on exiting the application, are automatically logged out of the system. In the

---

following paragraphs some consideration about security of operating system and application software are to be discussed.

D) System Software Controls
Definition:

Ritchie (2005) defines that, the term security is used to refer to all aspects of protecting a computer system from all hazards such as physical damage, loss or corruption of data, loss of confidentiality etc. so specific threats and their possible consequences can be summarised as follows:

* Physical Treats such as fire, flood, etc. and sabotage and machine faults that their effects are loss of availability of machine and / or data.
* Accidental Errors such as programmer error and user or operator error that their effects are corruption of data.
* Malicious misuse such as viruses, worms and corruption or destruction of software that their effects are corruption of data and software and loss of availability of hardware.
* Fraudulent misuse such as deliberate modification of data or software that their effects are financial loss.
* Unauthorised access such as accessing of confidential data that their effects could be related to specific to circumstances.\(^{20}\)

Therefore while computers became more sophisticated, many manual operations are automated within the operating system. Operating system is the system software that runs all other applications and conducts the undertaking of coordinating all tasks, such recognizing input from the keyboard and keeping track of files and directories. It also ensures that all the different applications that are running and the users for those systems do not interfere with each other. As other significant task performing through operating

\(^{20}\) Ibid. PP. 222-223.
system is security that no unauthorized use occurs. Some popular operating systems are Unix, Windows, etc.

Accordingly in the following a checklist showing controls over operating system in two section including Physical/ general security and logical security are presented as follows:

a) Physical/General security
* Determine if the security features have been enabled and parameters have been set to values consistent with the security policy of the organization such as availability of original license of operating system, operating system media and related manuals and user guidance issued and provided through EDP department or vendor in user departments and branches.
* The audit of operating system security requires the auditor to have a general information and a good knowledge of the various features of the operating system like system configuration like memory, size, version, etc., running of the latest operating system version. The audit of the evaluation of security parameters in the operating system involves logging into the system and seeing the values on the system or running a few commands to find these values.
* Determine if the access to the system through all users of the system (user IDs) have appropriate privileges approved by the head of user department and branch manager to the various resources and data held in the system. The auditor should obtain the list of user IDs that it must be kept in a register in user departments and branches in details including employee name, designation, employee number, date of joining, user ID allotted, date of creation of user ID, date of deletion of user ID, signature of the user, then the auditor has to determine for each user what the permissions and privileges to the different resources/data are in the system.
b) Logical Security

* Determine if the logical security that is related to the control of access to applications and data are in appropriate positions.

According to Ritchie (2005)\textsuperscript{21} mentions that “A password mechanism is often the first and most significant line of defence in a multi-user system. In order to gain access to the system, the user enters a personal identification name together with a password associated with that ID name. The password can be assigned by an administrator or devised by the individual user”. Some characteristics of a good password system are; a minimum password length, password history, password required, compulsory password aging, lockout on unsuccessful logins, login station and time restrictions. The other areas of scrutiny are whether the logging of certain events, such as unsuccessful login attempts, has been enabled or whether the appropriate person holds the super user password.

i) The system must require a password of at least 6 characters (alphanumeric digits) and to ensure this requirement, it should be through the password definition parameters incorporated in system verified that the password length is specified according to the EDP security policy of the Bank.

ii) The system must log all password attempts so that the maximum number of invalid logon attempts such as by a hacker are produced in the system according to the EDP security policy of the bank and also the system should allow only a limited number of such attempts (say, three).

iii) Shutdown of terminals when an incorrect password has been entered e.g. three times

iv) Passwords should not be guessed but should be easy to remember.

v) Regular and frequent change in password according to EDP policy of the bank.

\textsuperscript{21} Ibid. P. 227.
vi) Staff training to assure that the staff aware of the need for keeping passwords secret.

vii) Ensure that access to operating system command prompt is disabled for general users in the user department and branches.

viii) Whether access rights to system files, application executable program files, application data files, utilities, application parameter files, system/database configuration/initialisation files, etc. have been adequately controlled to allow read / write / execute / modify, etc. as the case may be to appropriately authorised users on need to know, need to do basis.

* Determine if access rights given to various users are appropriate. In other words, the auditor should see what data and systems are on the server and on the basis of their critical and sensitive nature, he/she should get an idea that proper staff with required knowledge and profession have assigned to each data and system. Besides application systems, many servers are used as file and print servers acting as a common repository for data for many users. In such cases, a review of the OS security to determine appropriate access for each user to his/her data is very important.

E) Application Software Controls

These controls are those designed to ensure that performance of EDP systems relating to recording, processing and reporting respectively for input, processing and output are adequately performed and data in various files (database) is accurate, complete and authorized so that an individual application such as opening an current account and debit and credit operation on it to reach correct balance runs smoothly and accurately and the data as life-blood of bank must be protected from loss, unauthorised use and change.

In the following the both kind of controls so that, first a short review is given to definition of that control and after, internal control checklist for that control that may be followed by auditors and inspectors of bank are presented.
a) Input Controls

Definition:
These controls are generally related to authorisation, conversion and rejection of input data that they must be entered, processed and in a form of output reported.

Checklist:
* Generally transactions are permitted to enter in the following forms, determine if they are properly approved and authorised.
  i) In the individually form through signature or stamp
  ii) In the batches form through user department
  iii) Through its own computer e.g. may a bank has set a limit on opening savings accounts for branches not less than $ 100 and this limitation is programmed to include authorisation limits not less than $ 100 on an exception report in which the opening of these kind of accounts is stopped.
* Whether user ID and passwords are adequate to prevent of entering unauthorised transactions?
* To control correctness and validation of input data in which entered and converted to readable form by computer, determine if edit errors are assessed and corrective action on the timely basis implemented.
  i) All fields must be completed with special character like alphabetical, numerical which by a computer can be read.
  ii) If an input to enter is subjected to a limit, it must be entered only up to that limit.
* To prevent edit errors some input controls may be provided such as:
  i) Missing data check to make it likely that all fields provided to enter data have been completed
  ii) Valid character check to ensure that all fields have been properly completed.
  iii) Limit (reasonableness) check to ensure that the limitation of entering data is considered.
iv) Valid check code to ensure that correctness of transaction codes with master list.  
v) Check digit to ensure that all identification number of accounts, employees, etc. have been correctly entered. 
* To ensure of correctness and accuracy of entering input data especially in batches uploading, determine if controls totals are properly assessed and corrective action is on the timely basis implemented. Controls totals are;  
i) Document control such as number of documents or records so programme sequence checks can be implemented. (It is numbering documents)  
ii) Hash totals such as employee or product number could be used to check that outputs are correct and complete. (They are meaningless and only as a control device that should not be added together)  
iii) Value totals that are used to check financial information that could be from source documents completed.  
* Does the software have adequate controls to ensure that, data have been accurately input e.g. range checks, validity checks, control totals, etc.  
* To modify a returned data determine if the controls are the same as original data.  
* Whether the source documents are kept for an adequate period of time.  
* Whether input data are only once and once to the system entered and accepted?  
* Determine if a transaction is rejected is through the system reported?  
* Verify if the inputs can be captured for various conditions. e.g. if signatures can be captured for single A/c, Joint A/c etc.  
* Having controls over entry of data in on-line systems to restrict access to terminals and to restrict data entry to authorized employees?
* On-line systems controls to prevent documents from being keyed into the system more than once and to permit tracing from the computer output to data source and vice versa?
* Determine if the rejected inputs and resubmission are properly and timely implemented.
* Determine if correction of input data in source documents are through user department done.
* Determine if correction of input data in the conversion stage are through EDP department done.
* Do controls exist over entry of data in on-line systems to restrict access to terminals and data entry to authorized employees?
* Do on-line systems controls exist, that prevent documents from being keyed into the system more than once, and that permit tracing from computer output to data source and vice versa?

b) Processing Controls

Definition:
These controls are generally related to control over the processing of inputs data in which have been entered in a computer system. It means when inputs data were entered into the computer system, through processing controls it can be ensured that the generation of data are accurate and processing of inputs data are as per pre-arrangement instructions incorporated in a particular programme (software) executed. The testing of processing controls could be done through a numbers of methods in where the most applicable once is, pre-programmed controls incorporated into the individual application software.

Checklist:
* Determine if computer applications includes the provisions such as accumulating controls totals to facilitate the balancing of inputs data with processing input totals for every run.
* Procedures within the data processing control function, providing proper control of data between the user and the EDP department?
* Controls over data entry; for example, to include adequate supervision, up-to-date instructions, key verification of important fields, and self-checking digits.
* Determine if the proper fields have been during the normal processing cycle utilized through:
  i) Attaching external labels (manual controls) to magnetic tape or disks to allow visual identification of a file
  ii) Internal files labels (an electronic controls) in the machine-readable for incorporate into the computer applications and so when an operator enters an identifier, the computer would read the internal label of the loaded transaction file and would reject it if the label was of the different identifier to that expected.
  iii) Generation dating to keep automatically keep track the current version of any particular file.
  iv) Run-to-run totals that allows verification of processing in each stage.
* In where the master file are those used by all runs of a particular kind of transactions so determine if master and standing data files are up to date, complete, accurate and authorisation procedure and segregation of duties are in proper and expected manner.
* Does the processing controls incorporated by applications in the system facilitate;
  i) Processes are not initiated out of sequences.
  i) Prevent of duplicate or missing transactions.
  iii) Prevent of errors that must be logically sound e.g. in the interest calculation process, generally, the user will run the interest run job and the system will take the customer balances (key data) and apply interest rates (key data) and debit/credit the interest. The program, which performs these activities, should be logically sound so that no processing errors are introduced.
iv) Adequacy of controls over the key data such as the rate of interest in savings account according the period of deposit, tax rate, etc. to ensure that the key data used as a basis for the generation of data are complete and accurate.

* Program controls over entry of data into on-line systems:
i) Editing and validation of input data.
ii) Data processing controls over rejected transactions.
iii) Controls for balancing transaction and master files.
iv) Determine if application maintains audit-trail to uniquely trace any modification/deletion/addition with user-ID.

* Determine if the application maintains adequate control over security items such as DDs / Pay Orders / Branch advices, etc. Are they reconciled and exceptions identified and reported?

c) Outputs Controls

Definition:
Output is the result of two earlier stages, means, in the first stage the inputs data are entered into computer system and processing them in the second stage, as outputs is reported. Output controls are also the result of controls of two earlier stages and if controls in the inputs and processing stages have been properly and adequately conducted, controls in the output stage are only confirmation of two earlier stages. Therefore in controls over output is to ensure that outputs are genuine, complete and accurate so output are handed over to those users (department and branches) who need them according to pre-determined design, so the outputs could support the required job.

Checklist:

* Review the format, contents, accuracy and utility of output generated by application to ensure that all items have been generated
* Review the adequacy of distributed outputs to ensure that handing over of outputs is according to the delivery schedule
* Whether generated outputs totals by the computer are reconciled against inputs and processing totals through data control groups and users (departments and branches).

* Does user department management reconcile output totals to input totals for all data submitted, reconcile the overall file balances, and review outputs for reasonableness?

* Are data in generated reports compared against the source of documents?

* Determine if the outputs (reports) are only delivered to authorized users.

* Determine the EDP stationery such as pre-printed cheque is by users department or branches accounted?

* Whether views of personnel as an executive opinion in department or branch is taken to see that the outputs are useful and otherwise corrective suggestions.

* Whether source of documents are retained by users for an adequate period of time to relate them to corresponding output records.

* Do user controls exist over rejected transactions through the use of a computerised suspense file of rejected transactions or an auxiliary manual system?

F) Database Controls

Definition:

Harnois (1991) says, Traditionally organisations maintained their records on ‘flat’ file. Each application had own separate files associated with it, and files were generally not shared by applications. While this approach worked well enough in small environments in where users did not share information and common information was not maintained in several different files, as the amount of data being maintained increased and the need to share information among departments became necessary to provide better customer service, this approach often resulted in high redundancy and inflexibility. It
became obvious that the better method of storing and retrieving information was necessary. Thus, database and database management system were developed. Basically, a database is a collection of logically similar records and provides the same data to everyone in the organisation having authority to access such data. It allows for multiple users and application access, reduce data redundancy, and facilitates maintenance efforts. In database system each piece of data is stored once, and only once, regardless of how many programmes or applications require the information. For example, if a bank customer has a checking A/C, savings A/C, a home mortgage and a car loan with the same bank, the customer’s name, address, social security number, etc. need only be entered and stored once. But in the ‘flat’ file approach, this information would be repeated in each of the four application files. While a database facilitate centralised control, multiple application access, and data independence and also reduce data redundancy, but some difficulties specially relating to the managing the database access process would increased. To cover such problem the database management system or DBMS were developed. DBMS generally provides the link between application programmes and the database by accepting functional request for data retrieval or update, locates data, performs necessary input/output and security checking, passes appropriate data and control information back to application programmes, and maintains its position in the data base, allowing it to progress logically through utilizing various products and utilities including a communication system and a data dictionary. To handle these above procedures, one or more database administrators are used. He is the manager of the database with responsibility for database design, definition, and maintenance and security and information classification.  

Roman (2005)\textsuperscript{23} defines that “a database is just a collection of related data. A database management system, or DBMS, is a system that is designed for two main purposes;
* To add, delete, and update the data in the database
* To provide various ways to view (on screen or in print) in the database”.

Checklist:
* Data Base Administrator (DBA) as a key responsibility for database and database management system (DBMS), determine if the responsibility of the DBA in the following areas is appropriate;
  i) Development and maintenance of the database
  ii) The security of the database
  iii) Maintenance of the data dictionary
* It is necessary to review security in the DBMS through a review of user IDs, the privileges associated with each ID and factors such as whether default-shipped passwords that are common knowledge have been modified/disabled.
* Determine the role of a data security officer in where a data security package is being used, and its role relative to database has been clearly distinguished.
* Determine if DBA periodically review the list of users to the database? Is the review documented?
* Are inactive users deactivated?
* Is there back up schedule?
* Determine if there is adequate documentation relating to standards in the following areas;
  i) Database design, maintenance and testing
  ii) Application design, testing, implementation and maintenance
  iii) Reorganisation and recovery requirements

iv) Protection and confidential data

* Determine if there is adequate documentation relating to database in the following areas;

i) A current data dictionary and data directory

ii) A list of data elements, record types, set types

iii) Access authorization

* Determine if authorized users are assigned specific access right based upon need and must be in written.

* Determine all terminal in which have the access to the database and determine the procedure to restrict the access to such terminals.

* Determine all media communication such as dial-up lines, satellite etc. procedure to restrict the access to such media communication

* Determine if the access to the system is restricted by confidential tool such as password

G) Internet Banking

Definition:

One of the greatest tool of banking services is banking online that also called Internet banking service. The term Internet banking refers to the use of the Internet as a remote delivery channel for banking services such as query on accounts balances, statement of accounts, cheque book request, demand draft request, bill payments, transferring funds to different accounts or electronic online payments so the customers can receive and pay bills on a bank’s web site. As a result, the bank’s customer can access their accounts or transfer their funds anywhere & anytime by using the Internet banking facility and hence the security of customer’s accounts, security of transaction performed through Internet Banking, security of bank’s system is the paramount concern. A bank can perform Internet activities in one or more of the following ways:

a) In informational level the Internet as a marketing tool by a bank to introduce its products to customers is used and risks associated with these operations are relatively low. There is no path between the
server and the bank’s internal network. This level of Internet banking can be provided by the bank or can be outsourced. While the risk to a bank is relatively low, the data on the server or web site may be vulnerable to alteration. Appropriate controls, therefore, must be in place to prevent unauthorised alterations of the data on the bank’s server or web site.

b) In Communicative level the Internet as an interactive tool between a bank and its customer is used. There is a direct path to bank’s internal networks in where the customer can take some banking services such as electronic mail, account inquiry, loan applications or static file updates (name and address changes). Here as compared to first level, the operational risk is higher and so controls should be in place to prevent, monitor and alert management of any unauthorised attempt to access the bank’s internal networks and computer systems. Virus detection and prevention controls are also important in this environment.

c) In transactional level, the Internet as a complete banking product is used to present the most kind of banking transactions that could be divided into two sections with a different risk profile. The basic transactional site only allows a transfer of funds between the accounts of one customer and the bank. The advanced transactional site provides a means for generating payments directly to third parties outside of the bank. This can take the form of bill payments via a bank official check or electronic funds transfer/automated clearing house entries. When the transfers of funds are allowed to a point outside of the bank, the operational risk increases. Unauthorised access in this environment can lead or give rise to fraud. Since a communication path is typically complex and may include passing through several public servers, lines or devices between the customer’s and the bank’s internal networks, this is the highest risk architecture and must have the strongest controls.

Therefore it must be reviewed the bank’s internal controls, policies, practices and procedures regarding electronic banking
activities with special attention to Internet banking. The following checklist would be useful to assess whether any potential concerns warrant further review.

Checklist:
* Determine whether the board, or an appropriate committee, approved the Internet Banking system based on a written strategic plan and risk analysis.
* Determine if management provides adequate training for all officers and staff affected by electronic banking systems, including those responsible for products, services, information systems, compliance, and legal issues.
* Determine if Internet banking is consistent with the bank’s overall mission, strategic goals and operating plans
* Determine if Internet application is compliant with the defined and approved business model.
* Determine if management and personnel of the organisation display acceptable knowledge and technical skills to manage Internet banking.
* Determine if measures to ensure segregation of duties are in place
* The bank has established policies governing the use of hypertext links such that consumers can clearly distinguish between bank and non-bank products, and that they are informed when leaving the bank’s web site
* There are appropriate procedures in place regarding change control, the review of audit trails and the review/analysis of usage logs (firewall logs and other reports)
* There are suitable and adequate procedures in place to ensure the privacy and integrity of the data and to ensure compliance with the applicable laws and regulations as well as best practice
* Information is provided on the web site to allow customers to make informed judgment about the identity and regulatory status of the bank before they enter into Internet banking services (name of the
bank and the location of its head office, the primary bank supervisory authority, ways to contact to customer service and other relevant information).

* Determine if updates and changes to the bank's public web site(s) only by authorized staff and subject to dual verification are made?
* Are web-site information and links to other web sites regularly verified and reviewed by the bank for:
  i) Accuracy and functionality?
  ii) Potential reputation, compliance, and legal risk?
  iii) Appropriate disclaimers?
* Determine if the bank operates the web site(s), electronic banking system(s) or core data processing system(s) internally and whether any activities are outsourced to a vendor.

**Identify the location of the following operations:**
  i) Design and maintenance of the bank’s public web site or home page.
  ii) Computer/server for the bank's public web site.
  iii) Development and maintenance of the bank’s electronic banking system(s).
  iv) Computer/server for the bank’s electronic banking system(s).
  v) Customer service (e.g., call centre) for electronic banking services.
  vi) Electronic bill payment processing or other ancillary services.
* There are appropriate incident response plans in place to manage, contain and minimize problems arising from unexpected events, including internal or external attacks.
* An information security architecture has been defined and is appropriate for the nature of the Internet banking model.
* The bank has an adequate process and controls to address physical security for hardware, software and data communications equipment associated with the Internet banking system.
* The bank has a sound process, which ensures adequate control over the path between the web site and the bank’s internal networks.
or computer systems and whether the internal network is suitably protected.
* Is the security infrastructure properly tested before using the systems and applications for normal operations?
* There are suitable and adequate procedures in place to ensure the identification of access points and potential areas of vulnerability
* There are appropriate manual balancing controls where automated controls are inadequate
* The record for each customer transaction contains identification of the customer, the transaction number, the type of transaction, the transaction amount and other information of relevance, if it is stored and archived, for control purposes or other business functions such as marketing
* Obtain a description and/or diagram of the Internet banking system and its capabilities. Consider hardware, software, points of connectivity to internal systems, and remote access points.

_Evaluate:_

i) How the Internet banking system is linked to other host systems or the network infrastructure in the bank.
ii) How transactions and data flow through the network.
iii) Potential areas of vulnerability.
* Obtain an overview of transaction and payment services flow and settlement process and determine whether:
  i) The bank's settlement responsibilities are clearly defined.
  ii) The vendor's policies address uncollected funds, settlement, customer service, backup, contingency planning, and disaster recovery.
* Determine whether the bank has established policies over hypertext links that enable consumers to clearly distinguish:
  i) Insured and non-insured financial products.
  ii) Bank versus non-bank products.
  iii) When leaving the bank's web site.
* Review a sample of Internet Banking customers and ensure they are only allowed access to accounts for which they are authorized signers.
* Have the policy necessary terms to report the following information to management periodically:
  i) Number of visitors to the website
  ii) Number and volume of new Internet Banking loans for the month
  iii) Number and volume of total Internet Banking loans as of the end of the month
  iv) Volume of total loans outside our normal servicing area
  v) Volume of total deposits outside our normal servicing area
  vi) All security threats or repeated unauthorized access attempts
  vii) Any time during which the Internet Banking site was non-operational for four hours or longer.
* Ascertain if an Internet Banking Security Officer has been named, as well as a backup.
* Determine that the bank has an adequate electronic banking security program that addresses the following, as appropriate:
  i) Access to, protection of, and disclosure of customers' confidential information
  ii) Methods for establishing the legitimacy of each party requesting an account action or submitting related instructions or data
  iii) What information may be shared with third parties?
  iv) The ability of service’s third party to access or monitor electronic transmissions between the bank and any of its customers.
* Determine if procedures are in place to control customer transfers of uncollected funds from each access point.
* Confirm that safeguards are in place to detect and prevent duplicate transactions within each system.
* For systems that permit access to credit lines, determine if draws or credit extensions are adequately controlled.
* Control features are in place to validate the identity of prospective customers while they use the Internet to apply for new bank loan and/or deposit accounts
* Authentication procedures are used to uniquely and positively identify the transacting party using digital certificates and digital signatures where necessary
* Determine whether adequate control features are built into the systems to ensure authentication of the user, data integrity, and confidentiality of transactions.
* Review customer comments, questions, and complaints logged since last audit. Ensure they were logged on the Customer Service Log and were handled timely.
* On a sample basis, determine if the following were obtained for new deposit accounts opened through the Internet Banking system:
  i) A credit check approved by an officer of the bank.
  ii) A review to determine if the account satisfied the bank's "Know-Your-Customer Policy."
  iii) If the account is foreign, a review of the Office of Foreign Assets Control lists of specially designated persons.
  iv) Signed new account application or signature card.
  v) A properly completed Internet Banking Account Services form (retail customers only).
  vi) Evidence that CD disclosures were mailed or faxed to customers.
* On a sample basis, determine if the following were obtained for new loan accounts opened through the Internet Banking system:
  i) Ensure no loan applications outside of the bank's normal trade area were approved to commercial customers.
  ii) A signed residential consumer loan application.
  iii) A signed note agreement.
  iv) Evidence that loan disclosures were mailed or faxed to customers.
* Ensure agreements / contracts are in effect for all Internet Banking customers.
* The network architecture is appropriate for the nature, timing and extent of the Internet banking operation
* The bank has an effective process to assess the adequacy of physical controls in place to restrict access to firewall servers and components
* Intrusion detection systems and virus control systems/procedures are in place
* Determine whether the bank has an adequate process regarding virus detection and prevention associated with the Internet banking system. Consider whether:
  i) User awareness efforts address viruses.
  ii) The virus containment program is documented.
  iii) Screening for viruses uses a virus detecting software package.
* The frequency with which anti-virus products and definitions are updated is adequate, and the most current version/release is installed.
* Virus detection software distribution is made through downloads from the bank's server.
* There is adequate penetration testing of internal or external networks
* The communication across the network is made secure using virtual private network (VPN) and related encryption techniques where appropriate and necessary
* Determine that written contingency and business resumption plans have been developed for failure of the Internet Banking system and/or communication lines.
* Review the backup policy. Determine the following:
  i) A policy exists that defines adequate backup frequency and retention periods for backup data.
  ii) The procedures relating to in-house and off-site storage of backup data and programs are adequate. Ensure critical backups are stored in a secure, off-site location. (Per policy, a backup will be made of
the Internet Banking system configuration files and customer configuration files daily. These files will be taken off-site.

iii) A test of the Internet Banking system backup files is made on an annual basis.

* Is each significant vendor, service provider, consultant, or contractor relationship involved in development and maintenance of the electronic banking services covered by a written, signed contract?

* Depending on the nature and criticality of the services, do contracts specify?

i) Minimum service levels and remedies or penalties for non-performance?

ii) Liability for failed, delayed, or erroneous transactions processed by the service provider and other transactions where losses may be incurred (e.g. insufficient funds).

iii) Contingency plans, recovery times in the event of a disruption, and responsibility for back up of programs and data.

iv) Data ownership, data usage, and compliance with the bank’s information security policies.

v) Access by the bank to the service provider’s financial information and results of audits and security reviews.

vi) Insurance to be maintained by the service provider.

* Determine whether Internet banking firewall policies address:

i) Responsibility for firewall maintenance and monitoring

ii) Well-defined access rules

iii) Access rules that dictate what traffic is allowed or forbidden.

* Determine whether encryption is adequately addressed in the security policy and the policy includes:

i) Who is responsible for control of encryption processes?

ii) How encryption is used.

iii) Data classification techniques.

iv) Use of encryption to protect transmission of passwords, messages, or data during internal and open network communications sessions.
* Determine whether policies establish the use of virus detection software and note the products used.
* Identify whether security policies are periodically reviewed and updated and note whether the board of directors or senior management committee approves the policies.

**5.4. COMPUTER-ASSISTED AUDIT TECHNIQUES (CAATs)**

In a computerised environment, some controls could be done through normal auditing procedures and tools, because they have physical existence or the computer produces visible evidence but in where the computer cannot produce visible evidence the manual tools could not applicable and some other tools are to be required. Generally there are two types of test of controls in Electronic Data Processing (EDP) System as follows:

5.4.1. Test of controls without the computer

This approach that is known auditing around the computer is similar to auditing in a manual system with the use of manual auditing tools in where the auditor is to be able to collect necessary evidences and evaluate them without the computer, sufficient to provide his auditing report.

5.4.2. Test of controls with the computer

This approach that is known auditing through the computer, is required in where the computer dose not produce the visible evidence and auditor or EDP system’s auditor could not through normal auditing tools collect and evaluate the necessary evidences that his report must based on. Therefore the computer as an auditing tool by EDP system’s auditor is utilised to collect and evaluate evidences necessary for providing his auditing report. Generally these auditing tools are known as computer-assisted audit techniques or CAATs.
Bhatia (2002)\textsuperscript{24} says, “CAATs are noting but a software. The software is either available off-the-shelf, or is specially developed. There are different types of CAATs available. The most widely used tool by the auditors to collect and evaluate evidence is the Generalised Audit Software (GAS). It enables an auditor to gain access to data and apply business rules (manipulate) to them in order to test the presence and effectiveness of internal controls.

Information systems have utilities, query language and report writing facilities. These are also the facilities required in conducting an audit. However, the auditors do not design these facilities for use. They can be utilised with extra efforts or IS skills and most of the auditors do not possess these extra IS skills. A special program or set of programs specially designed for audit is required and is called audit software”.

So in the following, first, a short review would be given to some of these categories of CAATs and next, the widely used auditing tool namely audit software would be described.

5.4.3. Some kinds of computer-assisted audit techniques (CAATs)

By far, in the auditing profession there has been many kinds of CAATs appeared so each of them presents new technique and required new skill and knowledge. In the following some of them are to be defined:

5.4.3.1. Working Paper Generation

To make automating working paper some packages like hard-coded and templates could be used. Hard-coded packages, which are based on Basic or C programming language and are highly structured with respect to input requirements and output formats. Templates that are based on some software packages like Lotus 1,2,3 or dBase

that facilitate some auditing function like Journal entry listings, Closing entry listings, Variance analysis, Ratio analysis.

5.4.3.2. System Analysis and Documentation Techniques

Auditors use these techniques for enhancing their understanding of systems and programs, including systems of internal control. These techniques provide powerful capabilities to help an auditor to gain a more thorough understanding of the relationships among flows of transactions and data, and the positioning of controls within systems.

5.4.3.3. Automatic Flowcharting and Flowcharting Packages

A special program that analyses the source code for a program of interest and then prints a block diagram of the key steps in the program performs automatic flowcharting. The resulting output may be more readable than the actual source code. While the auditor must still draw the initial flowchart, flowcharting packages provide tools to make this task easier than it would otherwise be.

5.4.3.4. Internal Control Modelling System

Generally a computerized questionnaire is used to record information about entity personnel and their functions, including information about who can access assets, who can access various records, and who performs control procedures. The system then evaluates the information recorded in the accounting system description against built-in criteria and summarizes potential control deficiencies for the auditor to consider.

5.4.3.5. Review of Program Logic

The auditor could obtain a detailed understanding of system processing by using this technique; however, program logic analysis, using program narratives, logic diagrams and/or source listings, is difficult and time-consuming. This method requires a good working knowledge of the programming language used and verification that the documentation accurately represents the actual object program used in the system.
5.4.3.6. System Testing Techniques

Auditors use these techniques for verifying the processing steps performed by systems and programs and drawing conclusions about the performance of systems or programs. i.e., input is created and run through a system and the output is then compared with predetermined results.

5.4.3.7. Test Data

Simulated transactions that can be used to test processing logic, computations and controls actually programmed in computer applications. Individual programs or an entire system can be tested. This technique includes Integrated Test Facilities (ITFs). Auditors can use test data for testing accounting processes and controls built into the system and programs such as on-line password and data access controls, edit and validation procedures, branching logic in transaction processing and complex calculations. Test data should normally contain both invalid data, to test error handling routines, and valid data, to test normal processes. Test data may be used for testing accounting procedures such as computations, postings, and automatic transaction generation routines, and for testing programmed controls such as computer editing of transactions, computation of control totals and arithmetical overflow, and validation routines. This technique is especially useful for testing of controls that leave no documentary evidence of their operation.

5.4.3.8. Integrated Test Facility (ITF)

This technique is an extension of the test data approach. The integrated test facility is often called the "dummy branch", because usually it is implemented as an extra branch in a system; for example an extra teller terminal in a bank. Using the ITF, a limited number of test entries are mixed in with the live transactions, processed by the entire systems, and then reversed manually, or by the ITF programs. Sometimes, the technique involves updating "dummy branch" master files.
5.4.3.9. Parallel Simulation

Parallel simulation or "program simulation" involves the use of a generalized computer software package to embody the major processing logic of the program to be tested. The feasibility of this approach depends largely on the complexities of the program being simulated and the capabilities of the package to simulate its logic; however, it may permit verification of complex processing in a fast and objective way. Spreadsheet packages are ideal for such simulations.

5.4.3.10. Generalized Audit Software Packages

They consist a computer program or series of programs designed to perform certain automated functions. These functions include reading computer files, selecting data, manipulating data, sorting data, summarising data, performing calculations, selecting samples, and printing reports or letters in a format specified by the IS Auditor. This technique includes software acquired or written for audit purposes and software embedded in production systems.

5.4.3.11. Custom-Written Audit Programs

The auditor, a programmer employed by the auditor, or auditee staff using conventional programming languages such as BASIC, COBOL, etc, develops the custom-written programs for special purposes.

5.4.3.12. Fourth Generation Languages (4GLs)

These techniques are not forced the auditor to take special EDP knowledge and have these advantages such as on-line documentation and instruction capabilities, allow rapid modification of existing routines, produce system documentation automatically, to designing screen layouts and reports, to program testing and use and have active data dictionaries which automatically update programs when data elements are modified.

5.4.3.13. Utility Software

Computer programs provided by a computer hardware manufacturer or software vendor and used in running the system.
This technique can be used to examine processing activity, test programs, system activities and operational procedures, evaluate data file activity, and analyse job accounting data.

5.4.3.14. On Line Databases

Many public databases are available which can be useful for audit purposes. For example, newspaper databases can be used for obtaining or maintaining knowledge of the enterprise; financial databases can be used for obtaining stock prices, and key industry statistics for use in analytical review; legal databases permit scanning of tax cases, court cases, etc. financial statement databases permit analysis of financial disclosure practices, etc.

5.4.3.15. Expert Systems

Expert or decision support systems that can be used to assist EDP system’s auditors in the decision-making process by automating the knowledge of experts in the field. This technique includes automated risk analysis, system software, and control objectives software packages.

5.4.3.16. Database Management Software

Database management software (DBMS) provides facilities for creating data files and then accessing their contents by using simple commands rather than writing programs. This software is particularly useful when a large number of records require to be maintained and periodically updated, or when different types of extractions and reports are required. DBMS can be used for storing client information, audit related data such as time data, details of confirmation results, etc. Several popular packages are available at relatively low cost for use with micro-computers (e.g., Dbase, Paradox, and Foxbase). Mainframe DBMS packages are much more expensive.

5.4.3.17. Communication Software and E-mail

With the introduction of portable microcomputers, data communication software is becoming increasingly important. Such software can provide a means for transferring data between mainframe and microcomputers, or between two microcomputers,
using regular telephone lines. In addition, the software usually provides facilities that convert the microcomputer into a terminal which can be used to access auditee computers (if they have dial-up capabilities), various public databases, or the auditor’s home office when he is at the auditee’s premises. Indeed, microcomputers have virtually replaced terminals as the means of connecting users to central computers. Electronic mail (E-mail) software is increasingly being used to help auditors to communicate. Most large accounting firms, industrial entities and public sector organizations have such systems in place. However, small firms can also take advantage of such facilities by subscribing to commercial services that offer E-mail services at a modest cost.

Accordingly Computer-Assisted Audit Techniques (CAATs) are important tools for the EDP system’s auditor in performing audits. As mentioned, they consist many types of tools and techniques in which may be used to perform various audit procedures such as tests of details of transactions and balances, analytical review, procedures compliance tests of EDP general controls, compliance tests of EDP application controls. Therefore it can be stated that the audit procedures including tests of controls (General controls and Application controls) and substantive tests (Tests of details and Analytical procedures) in a manual and EDP environment are the same but the tools and techniques are differ and in an EDP system such techniques mentioned above may be only way to extract data or create an audit trail in the absence of human-readable records.

To planning the audit using CAATs, the EDP system’s auditor should consider an appropriate combination of manual as well as EDP techniques. When CAATs are used, some factors such as computer knowledge, expertise, and experience of the EDP system’s auditor, availability of suitable CAATs and EDP facilities, Efficiency and effectiveness of using CAATs over manual techniques, Time constraints, Integrity of the EDP system, Level of audit risk must be considered.
To planning the audit of EDP system, some steps that should be undertaken by the EDP Auditor may be as follows:

* Set the audit objectives of the CAATs (Test of controls)
* Determine the accessibility and availability of the organisation’s EDP facilities, programs/system and data
* Define the procedures to be undertaken e.g. statistical sampling, recalculation, confirmation, etc.
* Define output requirements
* Determine resource requirements such as skills, tools, personnel, CAATs, processing environment, etc.
* Obtain access to the organization’s EDP facilities, programs/system, and data, including file definitions
* Document CAATs to be used, including objectives, high-level flowcharts, and run instructions

5.4.4. Generalized Audit Software (GAS)

Hayes et al. (2005) mention that Generalized Audit Software (GAS) packages contain numerous Computer Assisted Audit Techniques (CAATs) for both doing analytical procedures and statistical sampling bundled into one piece of software. There are widely used GAS packages such as ACL and Idea. GAS packages provide the auditors with the ability to access, manipulate, manage, analysis, and report data in a variety of formats. Using GAS in an audit requires converting client data into a common format and then analysing the data. This is referred to as file interrogation that the following six types of audit tasks could be accomplished;

* Convert client data into common format
* Analysis data
* Compare different sets of data
* Confirm the accuracy of calculations and make computations
* Sample statistically
5.4.5. Applications of GAS like ACL in Bank

In the following, control testing related to some banking activities, using ACL software as a sample useable through EDP system’s auditor could be as follows presented:

5.4.5.1. Asset management

* Analyse inter-company profit or loss on asset sales
* Show items depreciated to cost, and determine assets higher than cost
* Compare book and tax depreciation and indicate variances
* Sample (random or specified) assets for physical examination
* Compare useful lives of assets by category and compare costs over time
* Compute investment tax credits and compare to credits taken
* Recalculate expenses and reserve amounts using replacement costs
* Recap asset values, in dollar value order, by net or cost amount
* Select samples for verifying repairs and maintenance disbursements

---

27 Researcher’s Note: ACL Services Ltd. is the leading global provider of Business Assurance Analytics to the audit and controls professions and the financial management community. Our international customer base includes 90 of the Fortune 100 companies and over half of the Global 500, the Big Four public accounting firms, and hundreds of national, state, and local governments. ACL software solutions are delivered in multiple languages in more than 130 countries to over 150,000 licensed users through a global network of ACL offices and channel distribution partners.
© 2004 ACL Services Ltd. AS/B&F/E/280504, Printed in Canada. ACL Headquarters, www.acl.com, E-mail; info@acl.com (Visited on 25/01/2006)
* Analyse for duplicate asset listings
* Extract assets with useful lives or depreciation rates beyond set norms

5.4.5.2. Loans by bank or branch
* Analyse impact of past-due accounts, unearned income, accrued interest, etc.
* Analyse impact of write-off for loans with late payments or other criteria
* Calculate unearned revenues from interest, discounts, insurance, etc.
* Compare original collateral less depreciation to outstanding loan balances
* Compare unearned revenue with client balances and report differences
* Determine loans where more than a specific percent extended terms
* Extract and print loans where payments were less than the regular amount
* Identify accounts with balances exceeding credit limits by percent overage
* Identify loans over or under specified amount, terms, or interest rate
* Isolate delinquent accounts issued prior to a specific date
* Report trial loan balances by account, location, branch, dollar amount, etc.
* Segregate write-offs, bankruptcies, and summarize by percent, date, etc.
* Select sample balance confirmations and merge with verification letter
* Show loans with remaining payments that fail to amortize calculated balance
* Sort and summarize loans by type of security, purpose, class, credit rate, etc.
* Subtotal, total, and print outstanding loan balances by any categories needed

5.4.5.3. Investment securities
* Calculate average yield by investment type and show detail variances
* Calculate total accrued interest receivable by type of security, agent, etc.
* Compare computed interest to amount actually received on investments
* Compare dividends declared per published service to amount received
* Generate frequency distributions of market value, interest, maturity dates
* Identify investments for which no dividends or interest have been received
* Price investments by merging investments file with security pricing file
* Segregate securities that are outside certain investment grade parameters
* Select samples (random or specified) of investments for market value tests
* Select samples of purchases and sales since last audit for audit verification
* Test amortization of premiums and discounts by selected (re)calculations
* List users who can input a trade and create/authorize payment instructions or journals
* Analyse trading activity for market timing
* List firm account trades just prior to client account trades in same security (Front Running)
* Analyse account activities for excessive trading or churning or wash sales
5.4.5.4. Cash disbursements
* Extract cash disbursements by vendor/supplier for audit verification
* Extract disbursements by bank and date for zero balance account transfers
* Generate vendor cash activity summary for loan or payables management
* Identify check requests that exceed set or selected dollar amounts
* Reconcile inter-branch transfers by extraction or inclusion
* Report on check disbursements for unrecorded liabilities
* Sample paid invoices for manual comparison with actual invoices
* Selectively audit payables trial balance for selected vendors
* Stop overpayments by checking duplicate invoices with payment request
* Summarize cash disbursements by account, bank, group, vendor, etc.
* Summarize check register in order by dollar amount and vendor
* Identify missing, duplicate, void or out of sequence check numbers

5.4.5.5. Credit management
* Extract accounts with balances over credit limit and sort by any criteria
* Identify and list accounts past due for specified time, order by amount
* Recalculate and verify current month’s interest charges
* Select and print detail activity for auditing selected accounts

5.4.5.6. Real estate loans
* Examine real estate mortgage loan file for principal and escrow balances
* Extract and report on loans past due for specified days or other criteria
* Generate frequency distribution of loans by principal value outstanding
* Identify amount and dollar volume on non-performing loans in any sequence
Analysis of EDP Auditing System in Banks

* Print a schedule of pre-paid accounts in any order or selection

5.4.5.7. Savings and Demand Deposits
* Show accounts with address changes and reversals within a four-week period – loss account analysis
* Create reports or analyses required for changing audit requirements
* List balances by branch or in total in any order required
* Prepare frequency distribution by amount, interest, or maturity rates
* Show accounts with incorrect service charge credits or reversals
* Recalculate interest or service charges on accounts for audit checks
* Select a sample of new or closed accounts for detail auditing
* Select samples and print balance verifications by account
* Show accounts with low balance, incorrectly exempted from service charges

5.4.5.8. Trust Assets
* Check participants’ file for non-allowable data (age, seniority, gender)
* Compare securities purchased to securities stipulated in trust instruments
* Extract trust asset information based on any criteria
* Identify accounts to be verified for pension calculations, payments, etc.

5.4.5.9. General Accounting
* Calculate and sort percentage variances in accounts between periods
* Compare and summarize costs for special pay, overtime, premium, etc.
* Compare summaries by major account in any order (low high, high-low)
* Compare useful lives of assets by category and compare costs over time
* Generate receipts distribution to chart of accounts for ledger comparison
* Isolate deferred payments and compare to accrued amounts in ledger
* Produce detailed list of manual payments by amount or vendor for audit
* Provide a complete audit trail for all cash deposits, withdrawals, adjustments
* Provide a complete audit trail for all disbursements by branch, creditor, etc.
* Recap asset values, in dollar value order, by net or cost amount
* Reconcile inter-branch transfers by extraction or inclusion
* Report checks paid that do not match checks issued, by bank, by check
* Report entries against authorization records for new or terminated employees
* Report on assets, compare book and depreciated values, and show variances
* Show items depreciated to cost, and determine assets higher than cost
* Compare current and prior years files for auditing changes
* Sort and report cash by amount, branch, account, etc.
5.4.5.10. General Ledger
* Review GL ticket activity for authorized or value transactions
* Validate GL account footing
* Review suspense accounts activity for appropriate use
* Verify feeder systems data in a consolidated ledger
* Review suspense transactions activity for appropriate and timely clearing and offsets
5.4.5.11. Pension and other Trusts
* Scan and total the schedule of investments (year-end or year-to-date)
* Select samples (specified or random) of asset transactions for test or audit
* Select trust assets for auditing current market value
As a result it could be stated that, today EDP system auditors have been involved to do their duty in complex environment namely Electronic Data Processing (EDP) system in where the major tool of one is a computer system. Auditing of these system because of complexity is differ from manual system and some test of controls in EDP system can be done without the computer, but some other tests of controls must be done through the computer and for this purpose some software have been developed that are known as Computer-Assisted Audit Techniques (CAATs). As mentioned in the previous chapters, one reason (Hypothesis) upon which this proposed study has been based is regarding to usefulness of these new auditing techniques (Computer Assisted-Audit Techniques (CAATs)) in EDP system with special reference to banking system that by previous literature have never been or could be more discussed. In this chapter, the researcher struggled to give many discussions about auditing in EDP system with reference to auditing standards relating to such system and after, auditing techniques applicable to this system and to complete this chapter the result achieved that the Computer-Assisted Audit Techniques (CAATs) are useful for auditors, and today EDP system auditor must accept such techniques as a fact to perform his functions.

5.5. SUMMING UP

The job of an EDP system’s auditor in auditing of EDP system is involved to collect and evaluate evidence in which some are visible and others are not and he must use both auditing controls tools including those are applicable in manual system and those are applicable to EDP system like GAS. To do this function, traditional auditing knowledge should be improved to those skills according and necessary in utilising of Computer Assisted-Audit Techniques (CAATs). The CAATs should be utilised in auditing function as a fact and the EDP system’s auditor must with the use of computer involved to his function in EDP auditing system.