INFORMATION TECHNOLOGY AUDITING IN

BANKING SECTOR OF JORDAN

The previous chapter highlighted the internal control technology and audit practices followed in the commercial banking sector of Jordan. The banking sector observe sound and effective internal controls based on the legislative framework stipulated by the Banking Law of Jordan. The internal audit and internal check practices are robust, integrated and effectively capable to check any irregularities and deviation from the norms in the conduct of baking business operations. The internal control and audit practices, moreover, are commensurate to the internationally accepted audit standards and practices.

The banking business activities in today’s world are, however, dependent on the computerized information technology. Application of software for information technology has accordingly been introduced in the banking sector and the banks are rapidly and increasingly switching over to a computerized banking environment for their operations. The banking sector in Jordan has been further adapting itself to countenance various developments such as internet banking, e-money, e-cheque, e-commerce etc. as the most modern methods of delivery of services to customers.

This chapter is, accordingly, devoted to the study of computerization of banking services and establishment of Information Technology (IT) function as well as security controls applied in banking sector of Jordan. It discusses the various aspects of the use of information technology and internal audit procedures and practices within the information technology (IT) environment in the banking sector. The Information Technology (IT) internal controls for audit are of paramount
importance to banking business in order to ensure the confidentiality, integrity, authenticity and timely availability of information. Presented in this chapter are, moreover, the objectives, organization and the various other relevant aspects of internal control, for an IT function which are essential for safeguarding of assets, data integrity, technology effectiveness and technology efficiency in an information technology function.

**Information Technology Application in Banking Operations**

Information Technology has revolutionaries the banking business in Jordan. Computers are used extensively now in Jordan’s banking sector to carry out multifarious banking business activities. Software application covers a wide range of accounting and financial operations. Banks are dispensing deposits and payment services at the counter to their clients through the use of computerized software. Maintenance of customers individual personal accounts are totally computerized almost in every bank of Jordan. Customer’s signatures and other relevant data is stored in the software ledgers. As a result customers enjoy the facility of one-window payments called the ‘Teller Technology’. This facility is available within the premises of the bank.¹

**Automated teller machines**

The electronic banking has enabled the customers to have access to the cash from the banks round the clock through ‘Automated Teller Machines’ (ATM). These machines are installed not only within the premises of the banks but also additionally at various market and common places of importance and convenience to customers. The ATM not only provides access to get ‘All Time Money’ but also facilitates universal withdrawal of money any time, any place’. Regardless of customer’s
affinity of accounts with any bank, the customers can withdraw money from ATM’s at any time and at any place in the country by the use of their ATM cards.\textsuperscript{2}

Numerous other banking services emerging from the application of information technology in the banks of Jordan and have been provided to the customers are discussed below:

**On-line Banking Services**

On-line banking allows the customers to perform some specific banking facilities without requiring the customer’s physical presence at the bank. It enables the customer to perform all routine transactions through their traditional banks; such as:

- View account balances
- Access account history
- Transfer of funds between accounts
- Schedule future transfers
- Pay bills
- Schedule automatic recurring bill payment.

Very few banks through their on-line banking sites also offer the following capabilities.

- Account aggregation: View balances and market values of on-line accounts held at other institutions, including investments, credit cards etc.
- Send payments to individuals via e-mail.
- Trade stocks and mutual funds
- Track real time stock quotes
- Receive trust and stock statements on-line
• View images of bill statements, cheques and deposit slips.

Large banks of Jordan as well as foreign banks offer fully secure, fully functional online banking for free or for a small fee. Some smaller banks offer limited access, for example, one may be able to view only one’s account balance and history but not initiate transactions online. Sooner than later, as more banks in Jordan succeed online and more customers use their sites, fully functional online banking likely will become as commonplace as automated teller machines in the country.

When a customer signs up for online banking and designates the account to access online, the customer is issued a user ID and a temporary password via regular mail or e-mail or both, with instructions on how to use them to access the secure online banking portion of one’s bank site where one’s account information is available 24/7.

**Electronic Fund Transfer (EFT)**

Computerized electronic fund transfer services are common place in Jordan banking sector. EFT uses computer and electronic technology as a substitute for cheques and other paper transactions.

The function can be used to:

• Transfer money between accounts within one’s bank
• Make a payment on a loan within one’s bank
• Take an advance on one’s bank credit line
• Wire money to one’s account at another bank
• Transfer money from one’s account at another bank to one’s account within the bank.
Customer who elects and sign-up to use the transfer function, has to designate the transfer amount, from and to accounts, and when one wants the transaction to occur, i.e. now or on a future date. Some banking sites also offer an array of transfer tools that allow one to set or change recurring transfers, check the status of a transfer, cancel a pending transfer, and receive a transfer alert via e-mail when the transfer clears.

**TRADE SECURITIES**

This function, provided by Jordan banks, provides the authorized use of the site to purchase, redeem or exchange equity shares through the banks securities subsidiary:

This function can be used to:

- Purchase trade securities from one’s bank’s funds by transferring money from an account.
- Redeem fund shares via transfer into a deposit account.
- Exchange shares between fund accounts.
- Transfer from a brokerage account and a secondary bank account.

**PAYING BILLS ONLINE**

Today, more and more banking sector in Jordan are offering this free as an online service on one’s banking site. One only needs to register the accounts one wishes to pay from and the Payee’s account one wishes to pay to. Enter the account information once only and one’s private banking site will keep those accounts available until one removes them. One can always change the accounts from which
Chapter-V: Information Technology Auditing in Commercial Bank of Jordan

one wishes to pay one’s bills and add more payees as needed. One also is given the opportunity to receive one’s bills online.

An increasing number of larger national banks as also foreign banks in Jordan now offer electronic billing, or e-bills, and accept e-payments.

ELECTRONIC PAYMENTS

The most common mode of payment, especially for low value purchases, is by cash. However, in modern age of information technology, customer feels convenient to pay for high value purchase through electronic payment technology.

Banking sector in Jordan, like their counterparts in other countries, offer e-payment services for their customer’s open market purchases. The most popular form of electronic payments is by credit or debit cards.¹

(i) Credit Cards

Currently, on line shoppers use credit cards for a majority of their internet purchases. Banks issue credit cards to their customers. A credit card has a preset spending limit based on the user’s credit limit. A user can pay off the entire credit card balance or pay a minimum amount each billing period. Credit card issuers charge interest on any unpaid balance.²

(ii) Debit Cards

Debit cards are issued by the banks for use by customers for their commercial transaction in much the same way as a credit card. But fewer sites of banks in Jordan offer the facility to use debit cards.
Debit cards are not appropriate for small transactions and do not afford anonymity. The major problem with the debit cards is that they are very less secured than the most commonly used credit cards.  

(iii) **Smart Cards**

The smart card is the latest addition in the application of information technology in the banking sector of Jordan. The card promises secure transactions using existing infrastructure. Smart cards are credit/debit cards and other card products (health insurance cards, employee or student identification card, driving licence card, etc.) enhanced with microprocessors capable of holding more information than the traditional magnetic strip cards. Smart cards can hold significantly greater amount of data almost hundred times more than the magnetic strip cards. Smart cards are also not exposed to external physical damages. But they are more expensive to issue.

**ELECTRONIC CHEQUE PAYMENTS**

Electronic cheques are another popular form of payment. Most of the cheques based transactions are usually held between business and are practicable where the business organization is willing to invest in special hardware (normally an electronic circuit attached to a P.C.) to sign payments. Hardware encryption of the signature is secure as it will be difficult for hackers to steel keys stored by certification agencies. It is also assumed that banks have trusted relationship among them and the clearing house which settles the cheque payments.

The purchaser fills an order form, attaches payment advice (i.e. electronic cheque), signs it with his private key using his signature hardware, attaches his public key certificate, encrypts it using the vendor’s public key and sends it to the vendor.
The vendor decrypts the information using his private key, check buyer’s certificate, signature and cheque, attaches his deposit slip and public key certificate, encrypt and send it to his bank. The vendor’s bank checks the signature and certificate and send to the clearing house. On clearance, the amount is credited to vendor’s account and credit advice sent. The purchaser gets a debit advice.

**Electronic Wallet Payments**

The electronic wallet serves function similar to a physical wallet, holds credit cards, electronic cash, owner identification and owner address information at an electronic commerce sites check-out counter. Electronic wallets make shopping and payments more convenient. The customer click on items to purchase, and then click on their electronic wallet to order the items quickly.

**RISK EXPOSURE**

Electronic payment technology in use in banking sector of Jordan are exposed to problems as mentioned below:

- Digital documents can be copied perfectly and arbitrarily often,
- Digital signatures can be produced by anybody who knows the private key.
- A payer’s identity can be associated with every payment transaction.

Obviously, without proper control and audit measures wide-spread use of software base services of the banks are not viable. Hence, a properly secured application of information technology can provide better safety and flexibility in the use of banks services.⁸

The internal control and audit must, therefore, take care of the following to check errors, fraud and embezzlements.
• Payment authentication
• Payment integrity
• Payment authorization
• Payment confidentiality.

Information Technology: Internal Audit and Controls

Computerized operations and services as the foregoing brings out, play a large and significant role in Jordanian banks. They assist in maintaining accounting and other financial records as well as assist to process data, draw financial statements and provide important information for decision-making. But software based facilities are prone to abuse. Privacy and integrity of data is of great concern in computerized environment working, particularly for banking institution which are basically deposit accepting, credit granting and other money oriented operational institutions. Banks, therefore, control and credit computer based information technology because the cost of errors and irregularities that arise in this technology can be high. In fact, bank’s ability to survive can be severely undermined through corruption or destruction of its data bases; decision errors caused by poor quality information technology; losses incurred through computer abuse, loss of valuable computer hardware and software personnel; the high costs of some types of computer errors; failure to maintain privacy of individual persons; and failure to control how computer are used within the bank.9

The information technology audit and control function has therefore been established in banks both at the local level and at apex level in headquarters to safeguard assets, to maintain data integrity and to achieve technology efficiency.
NEED FOR INFORMATION TECHNOLOGY INTERNAL AUDIT

The major stimulus for establishment of information technology audit function within banking sector of Jordan has been provided by the necessity to check computer abuse. Parker (1976) defines computer abuse to be “any incident associated with computer technology in which a victim suffered or could have suffered loss and a perpetrator by intention made or could have made gain.”

Some major types of computer abuse that the banks are vulnerable to encounter include the following:

<table>
<thead>
<tr>
<th>Types of Abuse</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Hacking</td>
<td>A person gains unauthorized access to a computer technology to read, modify or delete programs or data to disrupt services.</td>
</tr>
<tr>
<td>2. Viruses</td>
<td>Viruses are programmes that attach themselves to executable files, technologies areas on diskettes, or data files that contain macros to cause disruption to computer operation or damage to data and program. They are designed to achieve two objectives: to replicate themselves and to deliver a payload that causes disruption of some kind.</td>
</tr>
<tr>
<td>3. Illegal Physical Access</td>
<td>A person gains unauthorized physical access to computer facilities e.g. they gain illegal entry to a computer room or terminal. As a result, they are able to cause physical damage to hardware or make unauthorized copies of programs or data.</td>
</tr>
<tr>
<td>4. Abuse of privileges</td>
<td>A person uses the privileges they have been assigned for unauthorized purposes, e.g. they make unauthorized copies of sensitive data they are permitted to access.</td>
</tr>
<tr>
<td>5. Destruction of Assets</td>
<td>Hardware, software, data, facilities, documentation or supplies can be destroyed.</td>
</tr>
</tbody>
</table>
6. Theft of Assets : Hardware, software, data or documentation or supplies can be illegally removed.

7. Modification of Assets : Hardware, software, data or documentation can be modified in an unauthorized way.

8. Privacy Violation : The privacy of data pertaining to a person or an organization can be compromised.

9. Disruption of operations : The day-to-day operation of the information technology function can cease temporarily.

10. Unauthorized use of Assets : Hardware, software, data, facilities, documentation or supplies are used for unauthorized purposes (e.g. computer time is used for private consulting purposes).

11. Physical harm to personnel : Personnel can suffer physical harm.

Administrative procedures and security control measures are effective in reducing the incidence of computer abuse and the losses incurred when computer abuse arises. These controls are especially important as the laws relating to computer abuse in Jordan are inadequate. In fact, the laws covering computer abuse in Jordan are still evolving. It is, thus, difficult to prosecute a perpetrator of an abuse because of loopholes that still exist in the laws.

**OBJECTIVES OF INTERNAL INFORMATION TECHNOLOGY AUDIT FUNCTION**

The internal IT Audit Functions in Jordan banking sector has been established with the clearly enunciated objectives that the computer technology checks the traditional computer related errors and frauds, ensures there are no computer abuses; safeguards assets, maintains data integrity, allows organizational goals to be achieved effectively and resources are used efficiently. The internal IT Audit function also
encompasses the technology effectiveness objective and the technology efficiency objectives. In a way, the internal IT Audit function supports external IT audit objectives also that specifically focus on asset safeguarding, data integrity and management objectives. Chart 5.1 below presents an overview of the objectives of internal IT audit function of the banks in Jordan.

**CHART 5.1**

Information Technology Internal Auditing

<table>
<thead>
<tr>
<th>JORDAN COMMERCIAL BANKS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safeguarding of Assets</td>
</tr>
<tr>
<td>Data Integrity</td>
</tr>
<tr>
<td>Technology effectiveness</td>
</tr>
<tr>
<td>Technology efficiency</td>
</tr>
</tbody>
</table>

1. **ASSET SAFEGUARDING OBJECTIVE**

The information technology assets of the banks include hardware, software, facilities, data files, technology documentation and supplies. Like all assets, they must be protected by a technology of internal control. Hardware can be damaged maliciously. Proprietary software and the contents of data files can be stolen or destroyed. Supplies of negotiable forms can be used for unauthorized purposes. These assets are often concentrated in one or a small number of locations, such as a single
disk. As a result asset safeguarding becomes an especially important objective for the banking sector of Jordan to achieve.\textsuperscript{13}

2. \textbf{DATA INTEGRITY OBJECTIVE}

Data integrity is fundamental concept in Information Technology Auditing. Data Integrity has certain attributes: completeness, soundness, purity, and veracity. If data integrity is not maintained, the bank no longer has a true representation of itself or of events. Moreover, if the integrity of a bank’s data is low, it could suffer from a loss of competitive advantage.\textsuperscript{14} Nonetheless, maintaining data integrity involves a considerable cost to the banks. The benefits, however, accruing from the data integrity exceed the cost of the control procedures adopted by the banks.\textsuperscript{15}

3. \textbf{TECHNOLOGY EFFECTIVENESS OBJECTIVE}

An effective information technology accomplishes its objectives. Evaluating effectiveness implies knowledge of user needs. To evaluate whether technology reports information in a way that facilitates decision making by its users, the internal IT Auditor must know the characteristics of its users and the decision making environment.\textsuperscript{16}

Technology effectiveness auditing occurs after a technology has been running for sometime. Moreover, the bank’s management gets its attestation through external auditor whether the technology is achieving its stated objective. This evaluation provides input to the decision on whether continue running the technology or modify it in some way.
4. TECHNOLOGY EFFICIENCY OBJECTIVES

Information technology consumes various resources: equipment, time, peripherals, technology software and labor. These resources are scarce and different application technology usually competes for their use. An efficient Information technology uses minimum resources to achieve its required objectives.

However, efficiency of any particular technology cannot be considered in isolation. Problems of sub optimization occur if one technology is ‘optimized’ at the expense of other technology.

Technology efficiency becomes especially important when a computer no longer has excess capacity. The performance of individual application technology degrades (e.g. slower response times occur) and bank customer can become increasingly frustrated. The banks management must come to know whether available capacity has been exhausted because individual application technology are inefficient or because existing allocation of computer resources are causing bottlenecks. The banks then decide whether efficiency can be improved or extra resources must be procured.

INTERNAL ORGANIZATION OF THE IT FUNCTION

The Information Technology (IT) function has been organized internally according to the major technology based activities that had to be performed by Jordan commercial banking institutions. Typically a centralized data processing or Information Technology Department has been established within banks. The department usually has a technology development group, a programming group, an operations group, a data preparation group and a general support or control group. The chart-5.2 shows the organizational set-up of the IT function in banks:
These groups are subdivided further. The programming group and technology analysis group are broken into a development group and a maintenance group each. The operations group is split into a computer operation group, network operations group and a library.

The designations, authority and responsibility structures have different levels in different banks. Moreover each Manager’s span of control is constrained to a small
number of immediate subordinates. Some of the typical jobs that are performed include the following.\(^{18}\)

<table>
<thead>
<tr>
<th>Job Title</th>
<th>Position Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Technology Analyst</td>
<td>Elicits information, requirements for new and existing applications, designs information technology architectures to meet their requirements; facilitates implement-action of information technology, writes procedures and user documentation.</td>
</tr>
<tr>
<td>2. Application Programmer</td>
<td>Designs programme to meet information requirements; codes, tests, and debugs programmes; documents programmes; modifies programmes to remove errors; better meet user’s requirements and improve efficiency.</td>
</tr>
<tr>
<td>3. Technology Programmer</td>
<td>Maintains and enhances operating technology software, network software and utility software, provides assistance when unusual technology failures occur.</td>
</tr>
<tr>
<td>4. Data Administrator</td>
<td>Elicits data requirements of the users of information technology services, formulates data policies, plans the evolution of banks data bases, and maintains data documentation.</td>
</tr>
<tr>
<td>5. Database Manager</td>
<td>Responsible for the operational efficiency of banks data bases; maintains access control over database; assists users to use database better.</td>
</tr>
<tr>
<td>6. Network Manager</td>
<td>Responsible for planning implementing, and maintaining data and voice networks.</td>
</tr>
<tr>
<td>7. Security Manager</td>
<td>Implements and maintains physical and logical security over the IS function; monitors the status of security over the IS function; investigates security breaches; assist users to design control; maintains access control mechanisms.</td>
</tr>
</tbody>
</table>
8. Librarian : Maintains library of magnetic media and documentation.

9. Administrative support clerk : Acquires consumables needed by IS function; registers and follows up users complaints, handles users enquiries, collates and distributes reports.

There is high degree of separation of duties within the Information Technology function. The separation of duties enables detection of errors and irregularities which otherwise would remain undetected. Separation of duties serves as an important means of reducing expected losses from unlawful events.

**LOCATION OF INFORMATION TECHNOLOGY FUNCTIONS**

The location of the information technology has a significant impact on its effectiveness. In case of banks which have an incessant flow of financial operations requiring utmost secrecy, integrity and accuracy, great significance is ascribed to the location of Information technology function. Since banking institutions are strategic organization – i.e. in which information technology are important to both the current operations and future operations, the banks in Jordan have a separate Information Technology Department that takes organization-wide responsibility for the Information Technology Function. As this Department has to be effective, it has been made independent of user groups. Accordingly, the information technology department is located at the Head Office of the bank with internet connectivity to each branch for data transmission with regard to all sorts of banking operations conducted at the branches. In the overall organizational hierarchy of the banks the Information Technology Function has been placed very high and this reflects the importance banks
ascribe to this function. The IT Function management has access to and influence on top management decision making.

INTERNAL CONTROL OF INFORMATION TECHNOLOGY

Top managers exercise control over the activities undertaken by Information Technology personnel primarily through the establishment and enforcement of policies and standards. Policies provide specific guidelines for behavior. Standards provide specific guidelines for performance. Both policies and standards are well documented, promulgated widely, reviewed regularly and updated promptly when the need arises. Moreover, frequent remindance of the staff is done by drawing their attention to the policies and standards that govern their work. Also, they are apprised of any changes to the policies and standards that affect them.

The Internal IT auditor ensures that the following standards have been established, promulgated and used. Existence of these standards also support the external IT auditor.20

<table>
<thead>
<tr>
<th>Type of Standard</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Methods standard</td>
<td>Establish uniform practices and procedures to be followed. For example, they govern how analysis, design, and programming practices are to be carried out and how technology is to be operated.</td>
</tr>
<tr>
<td>2. Performance Standards</td>
<td>Describe the resource usage that should be expected from undertaking different information technology activities and the quality of the results that should be achieved. For example, they specify the time it should take to test certain types of programs and the average response time that should be achieved with online technology.</td>
</tr>
</tbody>
</table>
3. Documentation Standards: Describe how the activities undertaken within and the technology developed by information technology functions are to be documented. For example, they specify the documentation to be provided with programmes that are prepared and the types of and quality of documentation that must be provided to the users of application technology.

4. Specific Function control standards: Describe the ways specific individual functions undertaken within the information technology function are to be controlled. For example, they specify the major check points at which reviews and sign-offs must be undertaken and the variance monitoring procedures to be used.

5. Post-Audit Standards: Describe the ways in which ex-post reviews of information technology are to be conducted. For example, they specify the make up of review team, the activities they must undertake and the form of the final report that must be prepared.

SPECIFIC INTERNAL CONTROL

In order to achieve the IS audit objectives of asset safeguarding, data integrity, technology effectiveness, and technology efficiency, the banks have set up a technology of internal controls. The control is a technology that prevents, detects, or corrects unlawful events. The overall purpose of controls is to reduce expected losses from unlawful events that can occur in a technology.\(^{21}\)

Preventive controls reduce the probability of unlawful events occurring in the first place. For this purpose the banks provide instructions on a source document which reduce the likelihood of the clerk who completes the document making an error. Detective and corrective controls reduce the amount of losses that arise if the
unlawful event occurs. If the bank clerk making data entry keys incorrect data into a computer technology, an input validation control detects that the data is in error and halts further processing. A small loss may arise from delayed processing, but larger losses associated with the corrupted database do not occur. In addition the control is able to determine the nature of the keying error made on the basis of past keying errors, and corrects the error without the clerk having to intervene. Thus the losses associated with recovering from the error are also reduced.

ROLE OF INTERNAL IT.AUDIT

The internal IT auditor’s task is to determine whether controls are in place and working to prevent the unlawful events that might occur within a technology. The chief concern of the internal IT auditor is to ensure that at least one control exists to cover each unlawful event that might occur. Even if an unlawful event is covered by a control, the internal IT auditor owes the responsibility of evaluating whether the control is operating effectively. Moreover if more than one control covers an unlawful event, i.e. redundant controls exist, the bank IT auditor has to ensure that all operate effectively. Otherwise, losses can be incurred because of reliance on a malfunctioning control instead of a reliable one.

As the IS internal audit is chiefly responsible to ensure the safety, validity, accuracy, completeness of transactions as well as technology effectiveness and efficiency, various internal controls are exercised. These controls are:

- General Controls in Information Technology set up.
- Application Controls in information Technology set up

These controls are briefly discussed below:
A. GENERAL CONTROL

The general controls are applicable to all types of computer applications and set the control environment in the banks. General controls consist of the following types of controls:

- Operating Technology Controls
- Technology Development Controls
- Technology Maintenance Control
- Data Management Controls
- Organization Structure Controls
- Computer Centre Controls
- Network Controls
- Personal Computer Controls

OPERATION TECHNOLOGY CONTROL: These Controls protect the integrity of the operating technology because it may face accidental threats as well as intentional threats. Accidental threats include computer hardware failures that cause failure of operating technology. Errors in user application programmes which operating technology cannot interpret also because operating technology failure. Accidental technology failure cause data destruction or cause whole segment of memory being dumped to discs and printer resulting into disclosure of confidential information.

Intentional threats to the operating technology are in the form of illegal and unauthorized access to, and use of data, for personal gains. IT audit functions provides protection against accidental threats through embedded technology software.
The protection against intentional threats of unauthorized access is protected through:

- Password
- Log on procedure
- Access token
- Access control list
- Discretionary access control

**Damage from viruses and other destructive programs**

Damage caused by viruses and other destructive programmes is more pronounced in computer network technology. Viruses affect the following types of files of a computerized technology:

- An EXE or COM program file.
- The OVL program file
- The boost sector of a disk
- A device driver program

These viruses and destructive programs can be grouped into four categories viz.

- Worm
- Logic Bomb
- Backdoor
- Trojan Horse

**Audit Trails for Security**

Audit Trial is the path which a transaction traces through a data processing technology from source document to summary reports. It refers to the procedure
which allows a transaction to be traced through all stages of data processing, beginning with its appearance on a source document and ending with its transformation into information on a final output document.

All audit traits are made use to support information security objectives of the following nature:

- Detecting unauthorized access
- Facilitating the reconstruction of events
- Promoting personal accountability

**TECHNOLOGY DEVELOPMENT CONTROL**

In the decentralized set up of Jordan banking sector operating with their branches located at distant places, technology development controls bring assume crucial importance. Technology development controls about uniformity in decentralized technology. These controls include the following aspects:

- Technology development authorization
- Technology development standards
- Control on technology development process

**TECHNOLOGY MAINTENANCE CONTROL:** These controls span over the Technology Development Life Cycle (SDLC). During this period, steps are taken to correct technology errors, to keep the technology current in view of the organizational requirements, and to update the technology when required. Technology maintenance activities have great potential for exposure to misuses. Therefore, the IT audit function develops and operates various maintenance controls to check technology misuse. These controls are of two types:
• Maintenance Authorization Controls

• Source Programme Library Controls

Maintenance activities increase the possibility of technology corruption, like logic corruption, programme corruption, data stealing, and so on. To check these corruptions, technology maintenance requires four controls: authorization controls, technical specification controls, testing controls and documentation controls.

Source Programs Library (SPL) Controls arise because of the following resources:

1. Access to programme is almost unrestricted Programmers and other person can have unauthorized access to the programs stored in library without detection.

2. Unauthorized changes can be made in any program, thereby reducing its integrity.

SPL controls overcome these problems. Use of SPL software controls four critical functions:

• Storing programs on source program library

• Retrieving programs for maintenance purpose

• Deleting obsolete programs from the library

• Documenting program changes to provide an audit trial of the changes.

**DATA MANAGEMENT CONTROL**

Data are valuable organizational resources for the banks. The internal IS audit function is responsible to manage it effectively, protect it carefully, and utilize it
efficiently. For effective data management the following effective controls are made by the banks.  

- Data access controls
- Data back-up controls

Data access controls are applied to prevent unauthorized individuals from viewing, retrieving, corrupting, or destroying the stored data. Such controls are required for data files when they are in use and when they are held in storage. Data can be accessed through terminals as well as by operators during production runs as data base is shared by many. Data access controls are made by bank IS audit function in the following forms:

- Defining user data domain
- Data base authorization table
- User defined procedures
- Biometric devices
- Data encryption

Data back up controls are designed to ensure that the bank can recover its files and databases in the event of data loss due to unauthorized access, equipment failure, or physical disaster. Back up controls result into creating original files and duplicate files known as back-up files.  

The back up technology makes a periodic back-up of the entire database. This is an automatic procedure which is performed by the banks at least once a day. The back-up copy is stored at a second place.
In order to ensure sanctity of databases banks adopts the following four methods:

- Regular back up: entire database is held on daily basis in a back-up copy which is stored in a separate secure place.

- Transaction Log: also called journal, keeps records of all transactions processed using database. These records provide audit trails of all transactions processed.

- Check point: Suspends all data processing and the technology remains in quiet state at a point where the technology reconciles the transaction log and database change log against the database. If a failure occurs, the technology restarts processing from the last check point. Thus, only a few minutes of transaction processing is repeated.

- Recovery Module: uses the logs and back-up files to restart the technology after a failure.

**ORGANIZATION STRUCTURE CONTROL**

Various information technology functions are organized by banks into a separate department and within the department each function is segregated from others. Segregation of functions significantly strengthens internal control as it seeks to divide responsibilities and assign tasks among peoples so that job functions do not overlap. It minimizes the risk of errors and fraudulent manipulation of bank assets.

Segregation has been done by the banks internal audit department in the following areas:

- Separation of technology development from computer operations.
Separation of new technology development from the maintenance.

Separation of database administration from other functions.

Separation of data library from operations

**COMPUTER CENTRE OPERATIONS CONTROL**

This control establishes procedures and methods to ensure that operations personnel follow correct procedures. These controls help to:

- Prevent or detect errors during data processing
- Prevent or detect fraudulent manipulation of data during processing
- Prevents access or misuse of personal or other classified information
- Prevent the destruction of record.

Computer operations controls are exercised by the internal IT audit department in the following manner:

1. Instruction for running computer jobs are fully documented, reviewed and approved by a responsible official of the bank.

2. There is arrangement for receiving data from user department/ branches, distributing outputs to them and establishing liaison with them to sort out information – related problems.

3. Schedules for input and output are prepared and relevant instructions issued to computer operators.

4. A log is kept of all errors and is cleared when data are corrected and re-input.
Computer hazard controls

In the Computer Centre the computer technology faces hazards of several types. These may damage the entire computer technology such hazards may be in the form of:

- Fire damage
- Water damage
- Power variations and failures
- Pollution damage
- Unauthorized intrusion

Disaster Recovery Plans

Appropriate measures have been adopted by the IT audit department in Jordan banks for controlling above hazards. Yet there are contingency plans also to meet any unforeseen hazard which ensure that normalcy would be restored within a time-limit after any disaster. These contingency plans include the following:

- Emergency plan
- Recovery plan
- Backup plan

COMPUTER NETWORK CONTROL

Computer networks are indispensable in the modern world. The banks in Jordan make extensive use of it in their organizations. Networks are quite popular in the form of intranet, extranet and internet. Communication networks work as communication sub technology which is responsible for communicating data to and
receiving data from different sub-technology in a technology or performing these functions in relation to other technology which are outside the bank organization.\textsuperscript{26} 

Internet provides to banks the following services:

- Communication
- Information retrieval
- World-wide web services

**Steps for computer network security**

The network security is exposed to two categories of concerns that infringe accurate and efficient data transmission. These are:

- Component failure
- Subversive threats

Component failure of any type may either block data transmission or result into destroying or corrupting data in the communication technology. Such a failure may also result into loss of databases and programmes stored on the network server.

Subversive threats arise when an intruder attempts to violate the computer technology. One can do it in two ways – invasive tap and inductive tap. In invasive tap, the intruder can read and modify data by installing any equipment in communication lines. In inductive tap, the intruder can monitor electromagnetic transmissions and read data.

**Control Measures for Network Safety**

The threats caused by component failure are overcome by banks through comprehensive proactive maintenance of various communication components. Such maintenance ensures that communication barriers are the least.
For overcoming subversive threats, comprehensive control methods are adopted by IS function of the banks which are in the following forms:

- Firewalls
- Encryption
- Message transaction log
- Call back devices
- Checking technology security

**PERSONAL COMPUTER CONTROLS**

In I.T. based bank operations, Personal Computers (PC) play vital role. Their use, however has also led to increased risks to the security of information technology. These risks include:

1. PCs are shift able from one location to another which opens the possibility that one can shift outside the organization with fraudulent motive.
2. Floppies are transportable and they can be taken away to steal valuable data of bank concerned.
3. Because of decentralized computing, chances of data corruption are high,
4. Failure of PC’s disc drive makes impossible the recovery of data stored on the disc.
5. Unauthorized access to PCs by intruders.

**Safety Measures**

The IT function department of banks adopts the following measures to overcome the above risks attached to PCs.
- Enforcement of physical locking of PCs and their keyboards.
- Storing of floppies at secured places.
- Floppy disc back-up
- Dual internal hard drives use
- External hard drives use
- Tape back-up devices use.

B. APPLICATION CONTROL

The Information Technology (IT) Audit Department of the banks also takes care of the computer application controls. The application controls are limited to input, processing, and output of various applications in the EDP set up.\(^{27}\)

Application controls accomplish the following objectives:

1. Completeness of input and update – to ensure that all bank transactions reach the computer and are recorded on computer files.
2. Accuracy of input and update – to ensure that data are captured accurately by the computer and recorded correctly on computer files.
3. Validity – to ensure that data are authorized and checked for appropriateness of transaction.
4. Maintenance – to ensure that data on computer files continue to remain correct and complete.

**Nature of Controls**

Application controls exercised by IT audit function fall into three broad categories:
(a) Input controls
(b) Processing controls
(c) Output controls

(a) **INPUT CONTROLS:** These controls prescribe procedures to check data for validity, accuracy and completeness when they enter the technology. Data input procedures are either direct (on-line) or source documents triggered (batch). In the direct input technology, on-line data editing techniques are employed to identify and correct errors immediately. The controls significantly reduce errors that may creep into the technology. Source document input requires more human involvement and is more prone to human errors. Dealing with such errors may require retracing the transaction to its source to correct errors.

Input controls are of the following types:

- Source document controls
- Data coding controls
- Batch controls
- Validation controls
- Input error correction controls

**Batch Controls** are used to reconcile output produced by the technology with the input originally entered into the technology. This is done to ensure that:

- all records are processed correctly
- no records are processed more than once
- an audit trial of transaction is created from the input through processing and output stages of the technology.
For batch controls, two types of documents are used:

1. Batch transmittal sheet
2. Batch control log

**Source Document Controls:** Technology that use physical documents to initiate transaction, controls are applied to these documents as these can be used to commit fraud. Computers will process the documents as they would appear legitimate. Even computers may prepare payment cheques on the basis of these fake documents.

Controls applied on source documents are:

- Pre-numbering of source documents
- Use of source documents in sequence
- Periodical audit of source documents

**Data Coding Controls:** Data coding is required to make data usable in computers. Two types of errors occur during the process of data coding:

- Transcription errors
- Transposition errors

Transcription errors are in the form of addition, truncation and substitution. Transposition and substitution errors occur when a digit or character in the code is replaced by another digit or character.

Data coding controls ensure that these errors are detected and corrected before the data go for processing. Following measures are adopted:

- Addition and truncation errors can be checked by the computer itself if the number of digits in a code has been specified.
• By use of check-digit method, substitution and transcription errors can be corrected.

**Validation Controls:** These controls aim at detecting errors in transaction data before these are processed. In computerized data processing, input validation occurs at various points in the technology. Some validation procedures require references against the current master file.

These are three levels of input validation controls:

• Field interrogation
• Record interrogation
• File interrogation

Field interrogation involves programmed procedures that examine the characters of data in the field. Some common types of field interrogation are limit checks, picture checks, valid code checks, check digit, arithmetic checks and cross checks.

Record interrogation checks data validity by employing sequence checks, formal completeness checks, redundant data checks, combination checks and password checks.

File interrogation ensures that correct file is being processed. It verifies that the file processed is the one the program is actually calling for. Two types of checks are applied in file interrogation:

• Version check – verifies that the version of file being processed is correct.
• Expiration date checks – ensure that the file is not deleted before its expiry.
Input Error Correction Controls: When an error is detected in a batch, it must be corrected and records re-submitted for processing. The error correction process is a controlled one so that errors are dealt with correctly and completely. Error correction is handled in three ways:

- Immediate correction
- Creating an error file
- Rejecting the batch

(b) PROCESS CONTROL

These controls aim at ensuring that data are processed correctly and data updating is accurate. Processing controls can be applied in two forms:

- Run Controls
- Operator Intervention Controls

Run Controls: Use batch figures to monitor batch as it moves from one procedure to another. Run controls ensure that each run in the system processes the batch correctly and completely. Specific uses of run controls are:

- Recalculating control totals
- Comparing transaction codes
- Sequence checking

Operator Intervention Controls: Allow operator’s intervention to initiate certain action, such as entering control totals for a batch of records; activating a programme from a different point in case of re-entering semi-processed records, etc. System that limit operator intervention are less prone to errors.
(c) OUTPUT CONTROLS

Output controls ensure that the results of processing are accurate, complete and properly distributed. If the technology output is lost, corrupted or misdirected, the organization has to sustain losses. Output controls are therefore needed. These controls are:

- Batch technology output controls
- Storage output controls
- Printed output controls
- Real time technology output controls

Batch technology are more susceptible to exposure and, therefore, require a greater degree of control than real time technology. In batch technology, once data are processed by CPU, these are transferred either for storage in storage media for subsequent retrieval or output is printed in the form of hard copy. Therefore, controls are required for both types of output. 29

Storage output controls are required to ensure that the EDP results are stored properly as well as the storage is of correct output. For this purpose, hardware controls, such as parity bit checking; and software controls such as check digits are carried out along with information output transmission to ensure that no digit have been lost in the communication process.

Printed output controls require verification of output, distribution of output and acting on exception reports. Verification of output is carried out in terms of input through a comparison between them where both are directly related or on the basis of previous relevant data when not directly related. When printed output is verified and distributed, the user departments also verify that they have received the correct output.
Real time technology does not produce hard copy of output but direct their output to the users’ computer screen or printer. The major threat to real-time output is in the form of interception, disruption, destruction or corruption of output during the process of transmission through communication network. The threat comes in two forms – equipment failure and subversive action of an unauthorized user. Preventive measures mentioned earlier are taken to overcome these threats.

I.T. EXTERNAL AUDIT PRACTICES

In the computerized environment of banking sector in Jordan, information systems are vulnerable to a large number of threats and abuses. Information system audit is very significant and of serious concern to the banks in Jordan.

Information Technology Audit Concerns

Concerns of IT audit of banks in Jordan ensure that following provisions have been made adequately:

1. An audit trail so that transactions can be traced forward and backward through the system.

2. Controls over accounting for all data and transactions entered into the system to ensure integrity of those transactions throughout the computerized segment of the system.

3. Handling exceptions to and rejection from the system.

4. Controls over changes to the computer system to determine whether the proper authorization has been given.

5. Authorization procedures for system overrides.

6. Testing to determine whether the system performs as stated.
7. Determining whether government directives, CBJ instructions, and banks policies and procedures are adhered to in system development.

8. Adequate controls between inter-connected computer systems.

9. Adequate security procedures to protect the users data.

10. Back up and recovery procedures for the operation of the system.

11. Data base are adequately designed and controlled to ensure that common definitions of data are used throughout the bank operations, that data redundancy is eliminated or controlled, and that data existing in multiple database are updated concurrently.

Areas of IT Audit

The broad areas in which IT audit is required are:

1. Overall Security

2. Program Development

3. Program Modification

4. Source Data

5. Processing

6. Data Files

STEPS IN AUDIT

The auditors in Jordan follow the general approach advocated by professional bodies of auditors, notably by the American Institute of Certified Public Accountants 1988b, 1990. The major steps undertaken by Auditors in conducting bank audit in Jordan are highlighted below:
1. Planning the Audit

It is the first phase of audit in which the auditor investigates the bank to determine the nature and requirements of engagement, assigning appropriate staff to the audit, obtaining background information about the client bank; understanding the client’s legal obligations; and undertaking analytical review to understand the client banks business policies and procedures better and identify areas of risk in the audit. Auditor also makes a judgement on desired level of audit risk acceptable to issue an unqualified opinion. The most important is the judgement on the level of control risks associated with each segment of audit. The internal controls of concern are Management Controls, general Controls and Application Controls. Auditors assess control risk in terms of each major assertion that bank management makes about material items in financial statements. In the case of application controls the relationship to financial statements is direct. If the controls have not been designed properly or not operated effectively, the potential impact on financial statement assertion is usually clear.

2. Tests of Controls:

In order to know whether the internal controls identified operate effectively, Auditors test internal controls. They rely on control tests as a basis for reducing more costly testing. Tests of controls, thus, evaluate whether specific controls are, in fact, reliable.

To test the controls, the Auditors identify a sample of programme they consider material to audit objectives. They examine the documentation for these programmes to determine whether, in fact, documentation exists and whether it complies with the standards. The auditor evaluates the reliability of application
controls by tracing instances of ‘material classes of transactions’ through each significant control exercised in various application sub-systems. For each transaction considered, auditors evaluate whether the control is operating effectively.

The external auditors tend to cut short the controls investigation when they identify control weaknesses and proceed to undertake expanded ‘substantive tests’ in light of the increased control risk they perceive.

After auditor have completed tests of controls, they again assess control risk. In light of the test results, they revise the preliminary assessment upward or downwards.

**AUDITING AROUND OR THROUGH THE COMPUTER**

In the control, testing phase, one of the major decisions auditor has to make is whether to test controls by ‘auditing around the computer’ or ‘auditing through the computer.’

‘Auditing around the computer’ is conducted only on the basis of input and output documents. The procedures and controls used in data processing as well as the programs and mechanism that transform input data into output data are ignored. The audit is performed by selecting a sample of actual transactions that have already been processed. These documents are traced from source documents to output records. If the source documents are properly reflected in master files and the output produced is correct, it is presumed that processing functions are correct. The manner in which processing is done, is of no consequence.

Under ‘Auditing Through Computer’, the auditor tests (1) the processing logic and controls existing within the system and (2) the records produced by the system.
The main tool used in this approach is the preparation of test transactions known as ‘test deck’. The test deck is run using the same set of programs and outputs are compared with manually prepared results. Test deck is created by simulating all possible conditions which can occur in input data.

**TESTS OF INFORMATION TECHNOLOGY**

IT Auditors apply tests on internal controls which enables them to evaluate the reliability, or operating effectiveness, of controls. The specific tests conducted on various controls are mentioned below:

(a) **Tests of overall security controls**

   Overall security control involves the following tests:

   1. Observation of computer site access procedures
   2. Observation of preparation and off-sight storage of back-up files.
   3. Review of records of password assignments and modifications.
   4. Verification of the extent to which data encryption is used.
   5. Verification of how unauthorized accesses are dealt with.
   6. Verification of effectiveness of data transmission controls.
   7. Verification of effectiveness of virus protection procedures.
   8. Verification of effectiveness of fire walls.
   9. Examination of results of tests simulations of disaster recovery plan.

(b) **Tests of Program Development Controls**

   Program Development Control tests involve the following:
1. Interview of users about their involvement in system design and implementation.

2. Review of minutes of development team meetings for evidence of user involvement.

3. Verification of management and user sign-off at milestone points in system development.

4. Review of test specification, test data and results of systems tests.

(c) Test of Program Modification Controls

Tests of controls related to Program Modification involve the following tests:

1. Verification of Information system management and user approval for program modification.

2. Verification that Program Modification documents and procedures comply with standards.

3. Verification that logical access controls are in effect for program modification.

4. Observation of Program modification in implementation.

5. Use of test for unauthorized or erroneous programme modification.

(d) Tests of Source Data Controls

Tests of controls relevant to source data are as follows:

1. Observations and evaluation of data control department operations and specific data control procedures.

2. Verification of proper maintenance and use of data control log.
3. Verification of how items recorded in error log are dealt with.

4. Examination of samples of source data for proper authorization.

5. Reconciliation of a sample of batch totals and follow up on discrepancies.

6. Tracing of disposition of a sample of errors flagged by data edit routines.

(e) Tests of Processing Controls

The following tests of processing controls are conducted:

1. Evaluation of processing control standards and procedures.

2. Evaluation of adequacy and completeness of data editing controls.

3. Verification that system output is properly distributed.

4. Reconciliation of a sample of batch totals and follow up on discrepancies.

5. Verification of processing accuracy for selected computer generated transactions.

6. Checking accuracy and completeness of processing controls using tests data.

7. Monitoring on-line processing systems using concurrent audit techniques.

8. Recreating selected reports to test for accuracy and completeness.

(f) Tests of Data Files Controls

Tests of controls for data files are as follows:

1. Observation and evaluation of file library operations, and file handling procedures by operations personnel.

2. Review of record of password assignment and modification.
3. Observation of preparation and off-site storage of back-up files, and of procedures used to control file conversion.

4. Verification of effective use of virus protection procedures.

5. Verification of use of concurrent up data controls and data encryption.

6. Verification of completeness, currency and testing of disaster recovery plan.

7. Reconciling master file totals with separately maintained totals.

(g) Audit Trail

Audit trail provides sufficient evidence matter to auditors and managers regarding the reliability and integrity of application system. It allows a transaction to be traced through all stages of data processing. The general procedure the auditor follows is to first investigate controls totals and run to run totals within the whole system and then to check and substantiate the audit trail by limited checking through records and files or by taking intermediate printouts of audit interest. In case of no provision of audit trail, the auditor in the report highlights this weakness in the IT system.

AUDIT REPORT

This is the final phase of bank audit in which the auditor, on the basis of the evidence provided by the result of control tests, formulate judgement (opinion) about whether material losses or account misstatements have occurred and IT system are effective and efficiency. The auditor issues a report and expresses the judgement reached in unambiguous manner. Audit Report may contain Disclaimer of opinion, adverse opinion, qualified opinion, or unqualified opinion.
CONCLUSION

The foregoing discussion concludes that the application of Information Technology Audit in banking operation in the banking sector of Jordan has been in wide use. All the banks now conduct their business activities in a computerized environment, and provide to their customers e-banking facilities. The information technology application has, in fact, enabled the banks to be compatible in doing the banking business with their counterpart banks the world over. Bank customers also now find it convenient to transact their banking operation efficiently through the electronic banking technology prevailing in the banks of Jordan. However, application of information technology exposes the banks that deal in money deposits and credit to various financial risks and other services hazards. It calls for information technology specific effective measures to check the errors, frauds, and ensure accuracy integrity, and security of data worked out and stored through electronic gadgets, I.T. procedures and technology. To this end, the banks have established Information Technology (IT) audit and control functions. A review of the IT audit function made in the study attests that the internal controls applied to check the abuse of information technology in the banks audit are effective. The controls exist at every step of the operation of technology and spread from the input point to the output stage. The bank has endeavored to make the IT function efficient and friendly to take care of the interests of their customer to their maximum satisfaction. The next chapter, accordingly, tests the IT function by eliciting the satisfaction levels of the bank customers in Jordan in the next chapter.
REFERENCE


5. Scott Bilker. Credit Card and Debit Management. Published by Press Pne Publishing. USA. 1996


9. L.M. Prasad, Usha Prasad. Management Information Control Technology. Published by Sultan & Sons, Delhi, India, 2009


