IT Policy

1. Need of IT Policy

1.1 The preventive IT Vigilance has to be seen now as a strategic management tool for carrying forward the Organizational objectives. An adverse IT environment is detrimental to the achievement of the Business goals in any Organization. Unlike Manual vigilance systems, IT vigilance has wider dimensions, because time and geographical distances are not constraints any more. All that is stored in a Computer is easily accessible from any site and at any time without the owner of the information getting to know what is happening in view of the complexity and sophistication of networks. While seen as a tool for business enabling, the Computer should also be viewed as a tool, which can cause havoc if not handled properly and hence suitable change is required in mindsets to foresee and formulate precautions.

1.2 Managing a system the way it should be, reduces the chance of a mishap. To be vigilant without having the basics in place, will defeat the very objective. Even fundamental deficiencies can create mammoth problems like misappropriations and frauds and it may leave us with controlling minor issues while the major issues will escape our attention. The better way towards avoiding such mishaps is to put in place a structured Preventive Vigilance mechanism, so that the users will have every opportunity to exercise the correct procedures and what is not followed will become exceptional for punitive vigilance to take care of.

1.3 Thus preventive Vigilance is of paramount importance to prevent a mishap from taking place at the very inception of a process.

1.4 Preventive vigilance can also be by way of *'watch and work'* by the officials in a branch. E.g. an official goes around the installation on a surprise visit and if any serious violations are found then the same may be acted upon immediately. *What is to be seen in* ***'watch and work'?***

a. Whether the users are using their own profile only?

b. Whether the passwords are written anywhere on the Computer Server, terminal,
printer, keyboard, calendar etc..

c. Whether the users leave their terminals in a locked status or logged out status
when they leave their seats temporarily?

d. Whether anyone other than an authorized user is using the computers?

e. The Server room is kept locked all the time?

f. Beverages etc., are not kept inside the Server room or near the PC?

g. Floppies or other storage devices are not kept on the desk of the users casually
without any controls?

h. Whether the Security personnel posted at the branch entrance is doing his duty as desired?

1.5 The application of computer and telecommunication technology has reduced the cost of entering new geographical markets, has provided for new products and enabled organizations to float a wider range of business models at frequent intervals. As the trend towards increased computerization is likely to continue for many years the quality of the computer systems/operations will decide the success of an organization.

1.6 Deficiencies in observation of security and control procedures relating to those systems/operations can pose significant threats to the efficiency of operations, effectiveness of results and success.

1.7 The threat is perceived to be from both the Internal and external sources, with historical reasons to believe, that the threat from the internal resources is more. Also, a dynamic attack from outside the Computer Systems say, through a network, can cripple the operations completely for some time. Hence the preventive vigilance plan has to tackle both these threats using the Technology and Procedures. This requires a comprehensive approach.

1.8 Continued lack of awareness of Preventive Controls will ultimately result in behaviour of some one intending to gain undue/dishonest advantage leading to computer frauds.

1.9 Hence it is essential to put in place extensive Preventive Vigilance controls, practice and review them periodically. This will reduce the tensions in the work place and will assure the users that they are in a safe and secure environment.

1.10 Some of the Preventive Vigilance aspects in a computer environment are given below

1.10.1 **To Prevent** - Unauthorized access to computers - software - data

a. Physical Access is to be restricted to authorized persons only in respect of Servers/PCs/Nodes/Workstations/Printers in a LAN Environment of a Computerized Branch.

b. Access to restricted areas to be electronically recorded or monitored during the Business hours/Non-Business hours.

c. Access keys/cards (like security cards and others) are tightly controlled and their use monitored.

d. Built in features like Login-ID/User-IDs and Passwords are essential controls at various levels of operations with time and date logs.

e. Forced change of passwords after a certain period

f. Limit the number of unsuccessful login attempts

g. Limit the concurrent connections by the same user

h. Security violations to be taken seriously and reviewed to avoid repetition.

i. Disable login IDs of transferred/terminated employees

j. Auto Locking of terminals after a certain specific interval of inactivity.

k. Restricted access to File Server.

l. Following areas of computerization are to be segregated to avoid manipulations, avoid unlimited access to computer resources and to ensure dual controls.

- Programming and Processing
- Programming and Data entry
- Programming and System Implementation
- Transaction Entry and Authorization
- Server Operations and Data Entry
- EDP Cell/Development Cell and Computer Security administration
- EDP and Computer Audit

1.10.2 **To Prevent** - Unauthorized modification to software - data*.*

a. Supervisory review over program changes/need should be sufficient

b. Proper documentation for changes made to programs.

c. Changed and tested programs to be placed in a protected interim library until they are reviewed by supervisory personnel.

d. Quality assurance team/function to review changes.

e. Enhancements to software to ensure compliance of requirements

f. Conversion of data to ensure data entry accuracy and completeness.

g. Supervisory Check to ensure data integrity after modification.

h. Pre - Image/Post Image of data changes to be kept in log.

i. Log to indicate that which user has used which program from what time to what time and from which node.

j. Maintain a proper Version Control of the software running at branches.

k. Ensure that the source codes of the programs are with authorized personnel only

l. Ensure that patch programs or correction programs are written only after its review by s Supervisory Authority.

m. Patch programs are valid only for a particular branch for a specific period only in order to prevent its misuse.

1.10.3 **To Prevent** - Unauthorized deletion of software - data.

a. Access to live source and object - code/data sufficiently restricted to prevent their
destruction.

b. Only ***copies*** of production programs are used for program modification.

c. The Backups of the following files are stored *off-site.*

- Source and object programs
- Master Files of data
- Transaction files and other files required for recovery

d. Programs/Data backups stored in Fire Proof Cabinets.

1.10.4 **To Prevent** - Unauthorized copying of software /Data

a. Original copies of software to be controlled by access restrictions

b. Physical Prevention of unauthorized copying of computer software

c. Inventory of all software to be periodically done and accounted for.

1.10.5 **To Prevent** - Accidental destruction of Hardware/Computer systems.

a. Protection from Fire, Flood, Burglary etc.,

b. Proper Annual Maintenance/Insurance to protect the systems

c. Preventive Maintenance to avoid Breakdowns

d. Maintenance of registers like Inventory, Errors and Breakdowns etc.,

e. Written emergency procedures to be in place for evacuation of personnel and critical files in case of fire etc.,

f. Terminals and printers are protected from destruction by outside influences

g. Insurance Policies to cover damages.

1.10.6 **To Prevent** - Unauthorized release of Information

a. Safe custody of magnetic - storage media containing customer data.

b. Restricted access to backup media containing data/information.

c. Floppies/Tapes to be locked and protected when being transported.

d. Floppies/tapes to be erased before they are reused.

e. Printed documents and reports (which are unwanted or no - more required) shredded if they contain sensitive information

1.10.7 **To Prevent** - Unauthorized transactions

a. Procedure to be in place to ensure physical/logical authorizations.

b. Only such Authorized transactions are processed and others rejected.

c. All transactions identified and tagged with the User-IDs with date and time stamp.

d. The system should prevent the same person who has entered the transactions to pass it or authorize it. This is to effectively introduce the dual control over such transactions.

e. To ensure only authorized persons originate/check the transactions, it should be ensured that menus/options appear on need to know and need to do basis.

1.10.8 **Preventive Controls to ensure redundancy - business continuity**

Most Important aspect of Preventive Vigilance is to build in appropriate redundancy into the system to ensure proper business continuity and to take care of contingencies such as,

a. Failure of Hardware protected through Alternate Server, Mirrored Disks etc.,

b. Malfunction of Software tackled by Backups

c. Loss of Data tackled by suitable backups - on-site, off-site, online, off-line backups
and documented restoration procedures.

d. Non-availability of trained Human ware by suitable HR policies/training to First
Line - Second Line - III Line System Administrator.

e. Failure of Communication Channels tackled by alternate channels - e.g., Leased
Line - ISDN Line - VSAT - one complimenting the other.

f. Failure of Site conditions - solution through Hot sites - Hot Standby - alternate Air
- conditioners, redundant UPS/power supply etc.,

1.11 Preventive Vigilance includes general controls as discussed above and environment specific selective controls for different computer environments. The underlying principle is to ensure prevention of frauds, operational efficiency and uninterrupted business continuity towards achieving organizational goals through computerization. The principles and practices of Preventive Vigilance should always aim at assessing *'what can go wrong'* and *'what controls it* and to put in place appropriate control mechanism with anticipation.

Environmental Controls

1. Introduction

1.1 Preventive Vigilance in respect of computerized branches starts with a proper environment for people to adjust themselves to the scheme of things being provided by the computers and the related operations. Whenever a computerized branch changes over from a manual environment to computerization, it is very important for all concerned to understand the various elements, the risks and the preventive controls and most important the implications in not following the controls.

1.2 Given below are some of the most common areas relating to computer environment, physical or otherwise, to tackle with.

2. Data Centre/Computer Room/Location/Access

2.1 Preventive Controls

2.1.1 For Data Center or Computer room creation standard laid down shall be strictly adhered by the bank.

2.1.2 The UPS and batteries shall be kept in a separate enclosure with proper locking facilities for prevention of unauthorized access.

2.1.3 There should be adequate space between the Computers and adequate moving space where computer systems are housed to enable proper servicing.

2.1.4 The Server room should be away from the glare of the public dealing places like the Banking hall.

2.1.5 Entry to the Data Centre/Computer room shall be strictly restricted and allowed only to authorized persons.

2.1.6 Printer should be placed in a separate room and not in the system room so as to restrict the entry of staff for collecting the print outs etc.

2.2 Implication in not observing the control(s)

Unauthorized access to Data Centre or Computer room may result in accidental *Switching Off* of the server/UPS, resulting in loss/corruption of data and delay in restoration/verification of data integrity resulting in business interruption.

3. Electrical Wiring/Data Cabling/UPS

3.1 Preventive Controls

3.1.1 Electrical Wiring to the Computer Systems is to be independent and direct from UPS. Except the Computer Systems and Electronic Equipment, it is not desirable to connect other electrical equipment to the UPS outlets - especially equipment such as Fans, AC etc.

3.1.2 There should be a gap of at least 1 foot between the Data cable and Electrical cables. They should cross each other only at perpendiculars. This is to avoid any possible electrical disturbances affecting 'data packets'.

3.1.3 Proper Earthling is to be provided to the UPS and Computers.

3.1.4 UPS Systems are to be housed in a separate enclosure and access to the room is to be restricted. Preferably, the batteries are to be arranged and kept separately in another part of the UPS room, away from the Main UPS equipment. UPS being an electronic equipment, may be kept in an Air-conditioned atmosphere wherever possible and the Batteries enclosure may be provided with an Exhaust Fan. No fire catching items such as old records, newspapers etc.. should be dumped in the UPS/Battery room. Sufficient moving space is to be provided around the UPS/Battery stack to enable easy maintenance by vendors.

3.1.5 UPS backup should be at least for the business hours.

3.1.6 The Car batteries emit heat and hence the room housing them is to be provided with exhaust fan. The Sealed Maintenance Free batteries (SMF) work more efficiently under Air-conditioned environment and hence the UPS and SMF batteries may be kept under AC environment.

3.1.7 All electrical points of the system should be labeled to indicate identity of the power switch connecting to various systems.

3.2 **Implication in not observing the control(s)**

3.2.1 Connecting Electrical Equipment like Fans and Tube lights may cause Surges and Spikes and are likely to cause damage to the Computer Systems.

3.2.2 Improper stacking of Batteries and dislocation may cause 'short circuit' and possible fire accidents.

4. Computer Assets

4.1 **Preventive Controls**

4.1.1 It should be ensured that all Computer Assets (Hardware and Software) as per sanction/supply are available in the branch and the assets are capitalized.

4.1.2 Computers, Printers, Switch, Routers, Modems and other peripherals connected with the Computer environment are to be numbered as per Fixed Assets Register. This register should contain the details of the systems such as their SR. No., Model No., brand name, supplier, original cost etc.,

4.1.3 Movement of Computer Assets from and to the Vendor's Place or between branches due to exigencies are to be properly recorded in a register.

4.1.4 There could be a procedure for periodic Hardware Audit as a part of the regular IS Audit. This could check the configuration details of all the Hardware supplied for agreement with the firm order placed by IT department on the vendor (Hard disk size, memory size, clock speed, OS version, Media/other drives, Monitor type, etc.).\

4.2 Implication **in not observing the control(s)**

4.2.1 Loss of control over the physical possession of the Computer Systems will result in unauthorized changes to the equipments/configuration and at times may result in loss of costly equipments.

5. Dust Protection

5.1 **Preventive Controls**

5.1.1 It is highly desirable to maintain dust free atmosphere in computerized branches.

5.1.2 Usage of Vacuum Cleaners and daily mopping of Computer Rooms, avoiding smoking, drinking and eating inside Computer rooms/near the Computer systems will all enhance the Dust protection. Eating and drinking inside the computer room/ATM room will attract rats, which may cut the wires and may lead to serious damage.

5.1.2 Proper sign boards/display boards will educate the users appropriately.

5.1.3 Overnight and when not in use the computer systems may be covered to protect them from dust.

5.1.4 Old Records and other articles are not to be dumped/stored near computer systems/UPS room.

5.2 **Implication in not observing the control(s)**

5.2.1 If proper dust free atmosphere is not maintained, the work culture will receive a serious setback.

5.2.2 The media like tape, floppies will get affected/unreadable causing loss of data

5.2.3 Frequent breakdown calls have to be made to vendors since the circuitry inside the computer systems, printers, drives etc., are very sensitive.

6. Air Conditioning/Temperature Control

6.1 **Preventive Controls**

6.1.1 It is desirable to keep the File Server room temperature under prescribed limits say below 22^0 C.

6.1.2 A thermometer may be made available in the FS Room to monitor the temperature.

6.1.3 Proper Air-conditioning equipment will take care of Temperature Control as well as Dust control.

6.1.4 UPS/Battery Room is provided with Exhaust FAN for proper dissipation of heat if car batteries are used.

6.1.5 UPS/Battery Room is provided with air-conditioned atmosphere if sealed maintenance free batteries are used.

6.2 Implication in not observing the control(s)

6.2.1 The electronic Circuitry and sensitive Hard disks are prone to damage in excessively hot atmosphere.

6.2.2 Efficient functioning is related to proper temperature control.

6.2.3 Improper AC atmosphere may cause frequent breakdowns.

7. Fire Protection/Water Seepage/Earthquakes

7.1 **Preventive Controls**

7.1.1 Appropriate Fire alarm systems, smoke detection systems may be considered wherever the risk due to fire is more.

7.1.2 Availability of proper Fire Extinguishers and proper training for its usage in a Computerized Environment are a must.

7.1.3 The respective vendors should undertake periodical servicing of the Fire Extinguishers.

7.1.4 Fire extinguishers should have proper validity period and should be refilled wherever applicable with date of refilling clearly marked on the fire extinguisher.

7.1.5 Use of Halon type of fire extinguishers, which might leave holes in the ozone layer, may be discouraged.

7.1.6 The Backup media is to be stored in a fire proof cabinet.

7.1.7 Water seepage from the ACs on to the UPS/server and other machines should be avoided.

7.1.8 Earthquake is a potential threat. Proper awareness may be created among all the people working in computer environment.

7.2 **Implication in not observing the control(s)**

7.2.1 Since the entire data and software are available in the Computer Systems, Fire can cause irretrievable damage. Restoration/Reconstruction of data with integrity is a very hard task and will result in enormous loss of time and human effort.

8. Storage of Floppies/Magnetic Tapes - Fire Proof Cabinet

8.1 **Preventive Controls**

8.1.1 Proper preservation of fresh/backup floppies/Tapes/Software CDs in a Fire Proof Cabinet away from the Main systems is a must.

8.1.2 Periodical testing of restoration should be carried out to check whether the backups are readable.

8.2 **Implication in not observing the control(s)**

8.2.1 Most of the times in a Computer Environment Media/Tape Backups of Data/Software are the only source available for restoration in case of destruction of original data/software due to fire/flood or accidental damages.

8.2.2 Hence if such copies are also kept along with the originals there is every possibility that such backups will become unusable.

9. Hardware Protection/Keys

9.1 Preventive Controls

9.1.1 The Hardware Keys provided to lock the Computer Systems will provide the necessary physical security. Leaving the Hardware keys on the systems overnight/when not in use will enhance the risk of misuse.

9.1.2 Hence it is desirable to keep the Systems physically locked and keep the keys in safe custody when not in use.

9.1.3 Also such keys should not be kept in open drawers, almirahs to prevent easy access.

9.1.4 Duplicate keys of the Hardware wherever provided are to be preserved properly.

9.1.5 A key register should be maintained and whenever duplicate keys are taken out it should be recorded.

9.2 **Implication in not observing the control(s)**

9.2.1 The keys form part of the critical elements for starting the systems for the day. If the same is misplaced it will delay the start of the systems leading to disruption in the functioning of the branch.

9.2.2 If the keys are left in the machine it self it may lead to unauthorized access and theft of keys may lock the systems permanently without alternatives.

10. Insurance

10.1 Preventive Controls

10.1.1 Electronic Equipment such as Computers, Printers, Modems, UPS and other peripherals are to be covered under *"Electronic Equipment Policy"* preferably with all risks covered comprehensively to take care of terrorism risk, earthquakes, burglary, theft, Malicious damage etc., for the replacement value of the systems.

10.1.2 Apart from this, the equipments are to be covered under Fire Policy "A" if the Electronic Equipment Policy does not cover *'Fire Risk'.*

10.1.3 Normally System Software Cost (Operating System) and Implementation charges are not to be included in the Insurance.

10.1.4 Since Premium on Electronic Equipment Policy is sizeable, avoiding the System software component will save a good amount.

10.2 **Implication in not observing the control(s)**

10.2.1 Insurance is a very vital contingency measure. In a computerized environment disasters to physical properties could take place due to multifarious reasons, such as lightning, short circuit, equipment breakdowns etc., Costly systems if not protected through insurance, will end up in loss due to huge cost involved in buying new equipment in replacement.

11. Annual Maintenance Contracts

11.1 **Preventive Controls**

11.1.1 Annual Maintenance Contract (AMC) is entered with the Vendors for the Computer Systems, UPS and peripherals and Air-conditioners to include Preventive Maintenance periodically and Breakdown Maintenance on call basis.

11.1.2 Normally AMC is entered after completion of the initial Warranty period (say 1 or 2 years from date of installation).

11.1.3 Likewise for the Application Software maintenance also AMC is entertained to enable modifications/enhancements to the software to suit User's requirements.

11.1.4 Only approved AMC charges are to be paid to the vendors and AMC charges should not be paid wherever "No service" is available.

11.1.5 Depending on situations the System Software cost and Implementation/ installation charges are to be excluded from AMC.

11.1.6 The items and extent of coverage under AMC should be agreed at the time of signing the agreement.

11.2 Implication in not observing the control(s)

11.2.1 If proper AMC is not in force, at times when Computer Hardware fails, service for repair will not be available immediately resulting in business disruption.

11.2.2 Application Software Bugs/modifications may not get fixed in time resulting in improper outputs/results and lack of good customer service.

12. Vendor Management

12.1 Preventive Controls

12.1.1 Vendor management is the most critical element for the success of ongoing computerization in a branch.

12.1.2 The names, addresses, E-mails, telephones etc., of hardware, software, data maintenance vendors are to be kept readily for taking up during installation, trouble shooting etc.,

12.1.3 Proper escalation procedures to be obtained and kept on record to take up with the next level of the vendor's organization in case the field level engineers do not respond or solve the problems to the satisfaction of the branch.

12.1.4 Periodical meeting of the branches and the vendors to be organized to sort out long pending issues and irritants.

12.2 Implication in not observing the control(s)

12.2.1 If proper vendor management is not observed, it will result in panicky situations, making desperate calls at the time of breakdowns.

12.2.2 Timely support will not be forthcoming.

12.2.3 Disruption to business continuity causing disruption in customer service.

12.2.4 Possible disputes between the vendor and the bank in the interpretation of obligations and service.

12.2.5 Substantial AMC charges paid will not be properly utilized.

13. Numbered Items like Deposit Receipts/Demand Drafts

13.1 Preventive Controls

13.1.1 In a computerized branch the usage of continuous stationery items for Deposit receipts/Demand Drafts/Bankers payment order etc., has become common due to printing of the items getting automated. This brings in new dimensions of risk of easy tampering since exposed from safe custody. Hence proper control over such items has to be monitored always and during the begin day and end day to ensure the numbers fall within the correct range.

13.1.2 A register usually called a securities issued register should be maintained to record the serial numbers of the above securities issued which will be kept with the appropriate authority usually the head of the division/department. However, the system at the end of the day should throw out a report as per the serial number of the securities so that the same can be checked with the securities issued register so that all the forms issued are accounted for.

13.2 Implication in not observing the control(s)

13.2.1 Loss of numbered items will lead to manipulations/misuse.

13.2.2 It poses restlessness and accountability factors.

13.2.3 May result in frauds.

14. System Software/Application Software - floppies/CDs/Tapes

14.1 Preventive Controls

14.1.1 Along with the Computer Systems, the vendors supply Original Set of System Software Floppies/CDs and other utilities. Such original sets should be preserved carefully and should not be allowed to be pirated.

14.1.2 Like wise, one set of approved version of the Application software is to be preserved either as a Media backup or tape backup. These backups are used in case of contingencies like disk crash, system restoration etc.,

14.1.2 Unauthorized copying of Original Sets of Software is to be prevented through necessary dual manual controls.

14.1.3 Along with the Original CDs/Floppies containing Operating system, etc., the floppies containing different device drivers for printers, Ethernet cards, pass book printers, modems, CD-ROM drive, anti virus etc., also should be maintained in the branches after recording in a register.

14.1.4 These floppies/CDs should be kept safely and also in a retrievable form.

14.2 Implication in not observing the control(s)

14.2.1 Preservation of Original Floppies with proper registration Number/License Number is a prerequisite for protection under Copyrights Act and other relevant Acts. Hence allowing them to be pirated will lead to complications.

14.2.2 Also the original floppies/media is needed for restoration of the operating system/drivers in case of disk crash/malfunctioning of systems and peripherals.

15. Manuals/Book of Instructions

15.1 Preventive Controls

15.1.1 Manuals of Various kinds are available in a computerized Environment.

15.1.2 Original Sets of Manuals for the Operating System and OS utilities, Printers, Modems, Inter-connectivity Hardware etc., 15.1.3 Original Sets of Manuals for other Utilities like office automation software, Anti Virus Software etc.,

15.1.4 User Manuals supplied by the Vendor for the Application Packages.

15.1.5 Manual of Instructions.

15.1.6 Desk Cards on Preventive Vigilance may be designed and provided to all the employees as a Staff Information System which will inculcate necessary awareness among the staff and the message of *"Prevention is better than cure"* will spread.

15.1.7 Preservation of these Manuals properly in the Branch Library is an important preventive control.

15.2 **Implication in not observing the control(s)**

15.2.1 The System Manuals are required frequently at the time of installation and when troubleshooting is done. Hence misplacement of the manuals will lead to lack of information, delay and business interruption.

15.2.2 User Manuals contain important information relating to operations of the application software and menus. Lack of manuals will lead to unorganized working.

16. Obsolete Computer Systems

16.1 **Preventive Controls**

16.1.1 Switch over to new systems and up gradation to the new technology may be planned well in advance with due analysis of Cost versus Benefit.

16.1.2 Standby Systems wherever provided (like Secondary Server, Spare Nodes,) should always be kept in working condition.

16.1.3 Spares from the Standbys are not to be removed for use at other systems.

16.1.4 There should be a policy for disposal of old/obsolete computer assets by way of buy back offer or otherwise.

16.1.5 Central Office from time to time taking into consideration the hardware obsolescence aspect should lay down the policy of replacing the systems like buy back arrangement.

16.2 **Implication in not observing the control(s)**

16.2.1 Due to advancement in technology, the computer systems may become obsolete and unserviceable due to lack of availability of spares.

16.2.2 This will result in delay in servicing due to unusable Hardware and possible business interruption.

16.3 Conducive environmental conditions are essential prerequisites and form the backbone for carrying out business with continued success under a computer environment. Hence all the preventive controls need be observed without exception and proper awareness on this has to be created among the various personnel concerned.

Information Systems Audit (IS AUDIT) and Computer Aided Audit Techniques (CAAT)

1. Introduction

1.1 One of the vital aspects of computerization is the IS Audit review of the existing practices in computer/networking environment and suggest such preventive measures required to curtail procedural violations and frauds. In this regard IS Audit (Information Systems Audit) plays a vital role in checking the deviations even at the source, thus preventing major mishaps. The role-played by IS Audit as a preventive vigilance tool is discussed below.

1.2 IS Audit by definition is the process of collecting and evaluating evidence to determine whether a computer system,

a. Safeguards Assets,

b. Maintains Data Integrity,

c. Achieves organizational goals effectively,

d. Consumes resources efficiently.

2. Assets

2.1 A computer environment possesses the following Assets viz., Hardware, Software, People, Cash/funds, Data Files, Information System Documentation, supplies etc., There must be an internal control system to protect and safeguard these assets from malicious damage, misuse, abuse, unauthorized access, (physical/logical), piracy of software, Computer virus and loss due to theft, fire, flood etc.

3. Data

3.1 Data is the 'Watchword' in a computer environment. It holds an exalted position in a computerized environment in that its real value is felt only when it is lost or damaged. Damage to vital data may cause irretrievable loss of prestige and loss of face to an organization. In a Banking environment where Banks deal with customer's money, protection of data is not only a necessity but also a legal requirement. Hence the concern for protection of Data is very high in any organization, especially banks. One of the major considerations of IS Audit is to assess Data Integrity, viz., its completeness, accuracy and veracity.

4. Effectiveness

4.1 Any computer system must accomplish its objectives effectively. In other words it must report information in a way that facilitates correct and speedy 'Decision making' by its users and organization. The effectiveness is ensured during the design stage and sometime after the system is implemented. An effective system should aim at improved productivity, improved work environment, ease of use, user satisfaction, state-of-the-art technology and benefit commensurate with cost.

5. Efficiency

5.1 A computer system is said to be efficient if it consumes minimum resources to achieve its required output. Some of the important resources are consumables, machine time, systems, peripherals, channels, software and manpower. It is difficult to strike a balance between cost and efficiency and evaluate optimum utilization of resources for obtaining greater efficiency. IS Audit may assist in this evaluation.

6. Preventive controls - Audit perspective

6.1 Given below are a few key areas of concern addressed during Information Systems Audit.

6.2 Access

a. Who can Access ?

b. What can be accessed?

c. How Access is controlled ?

Example:

1. System Administrator's access is controlled by his User-ID and Password.
2. Application User can access only predefined menus through respective User-IDs and their Passwords.

6.3 Authorization

a. What Needs authorization?

b. Who should authorize?

Example:

1. Funds passing in respect of TODs to be authorized by Branch Manager.
2. Levels of authority and Passing Powers of: Asst Manager, Manager, Senior Manager, Chief Manager

6.4 Accuracy

a. Data

b. Program Logic

c. Reports

6.5 Auditability

a. What evidence system provides to help Auditing?

Example

- Well formatted **Audit Trails.**
- **Access** Logs.
- **Transactions** linked to User **IDs.**
- Well formatted transaction logs.

- Error Logs.
- Well structured Reports. Detailed Product Reports.
- Cash Scrolls, A **and** L, P **and** L.
- **Use and** Compatibility of Audit Software Audit Through the Computer

7. Types of Controls

7.1 Following are some of the major controls being reviewed during Information Systems Audit:

7.2 **Directive controls**

a. Management policies
b. Guidelines and circulars
b. Books of Instructions and Manuals

7.3 **Preventive Controls**

a. Password and user-identification
b. Segregation of duties
c. Hardware locks
d. Version controls
e. Check digits
f. A well defined computer security policy
g. Creating security awareness
h. Provision of disciplinary measures for security violations.

7.4 **Detective controls**

a. Range checks and sequence checks
b. Printouts of reports
c. Exception reports
d. Checksum generation
e. Audit trails and Access logs
e. Transaction Logs

7.5 **Corrective controls**

a. Reconciliation and matching
b. Balancing of accounts
c. Interactive display and correction of errors
c. Enforcing disciplinary measures for security violations.

7.6 **Recovery controls**

a. Backups

b. Off-site storage of duplicates

c. Checkpoints

d. Transaction listing

e. Recovery and Restart (Contingency planning)

8. Role of IS Auditors

8.1 The role of the IS Auditor is a supporting one in smoothly and systematically implementing computerization in a bank. Unlike a traditional auditor, the ISA is perceived as a counselor in the process of computerization and specifically in critical stages such as system design, system development and implementation.

8.2 His thrust is towards better security, adequacy of internal controls, review of manual controls vis-à-vis system imposed controls and a judicious mix of them.

8.3 While the developer of the software is concerned about the flexibility, the IS Auditor is more concerned about controls. Where there are watertight controls and security is more the response becomes slow and ultimately the user of the system and the customer service suffer.

8.4 Where there is more flexibility it will help exploitation of loopholes leading to undesirable consequences and Computer Frauds.

8.5 Judicious mix of 'flexibility' and 'security' is to be ensured to provide services without dilution of essential controls.

8.6 While reviewing the system either during pre-implementation or during post implementation IS Auditor must keep in mind that 'he should not introduce any system of internal control afresh on his own'. However he may add any suggestions to his report to enable consideration.

9. Approaches

9.1 The two types of approaches to IS Audit are.

a. Audit around the computer

b. Audit through the computer.

9.2 **Audit around the computer**

This method follows a traditional approach in that it does not call for high technical skills and is mostly confined to verification of output results with the given input and in case of erroneous output the input is checked for consistency.

9.3 **Audit through the computer**

This method requires a high degree of computer knowledge and skills and calls for a professional approach. In this approach the process logic (programs) of the computer is checked in Toto with the Input and Output.

9.4 **Frequency of Audit**

Audit of computerized systems is not a one-time job. Security audit should be conducted periodically at irregular intervals with a periodicity specifically determined for different types of sensitive systems.

10. Stages of Audit

10.1 Migration Audit

Migration audit is taken up at the time of switching over from either manual to computerized system or from change over from one platform to another under computerized set-up. Procedures for migration audit includes verification of master data, transaction data, account balances, etc. before and after migration to ensure completeness and accuracy of migration. This should cover system parameters and codes, which govern the functioning of the application.

10.2 Pre-Implementation Audit

a. During development of software stage - participate in the system design process to recommend system quality in the areas of security, audit controls and operational continuity.

b. Review the system environment and the related manual procedures to ensure standards (uniformity of procedures) in the areas of Design - Documentation - Programming - Testing

10.3 Post-Implementation audit

The following reviews are conducted during Post-Implementation Audit.

a. Environmental Review

Review of: Installation, place, machines, Air conditioning, Warranty/AMC/ Insurance, personnel, preservation of documents, training needs etc.,

b. Operations Review

Computer operations, exercise of manual controls, authorizations, physical access controls, transaction inputs, retrieval of outputs etc., Operations review should include security audit of remote terminals of the systems as well. The efficacy of centrally controlled software access controls must be tested.

c. **System software/Application software Review**

This includes Operating system review, firmware review, application program review, source code review, testing etc.,

d. **Disaster recovery and contingency planning**

This is concerned with the computer security/frauds (preventive and post review), uninterrupted customer/business services, back up procedures followed, effectiveness of backups, restoration procedures, disaster recovery and fallback procedures in case of natural disasters like flood, fire, cyclone, earth quake etc.,

11. Prerequisites

11.1 Before proceeding with IS Audit of a Computerized Branch/Office the IS Auditor should be familiar with the following.

a. Overview of Computer Operations and connected entities.

b. Management Guidelines with regard to Computerization.

c. Systems and Procedures specific to Computerized Branches.

d. Bank's Procedures and Instructions with regard to various Application Packages.

e. Legal aspects relating to Banking Operations and Statutory obligations.

f. Comparison between Manual Procedures vis-à-vis Computerized Procedures and Change Management.

g. Duties and responsibilities of various Computer Personnel viz., System Administrator, Supervisory Users, Operators

h. Risk, Concern and Internal Controls specific to Computer Environment.

i. IS Audit Guidelines and Checklist.

j. Scope and extent of IS Audit.

k. Reporting Format.

12. Assessment

a. Observation of Activities

b. Procedure stipulated.

c. Desired Control to be exercised (Wherever controls specific to any activity is not prescribed).

d. Violation/Deviation/Irregularity/Lapses

e. Absence of control explained to the System Personnel/Branch Manager for immediate corrective action

f. Effect on the system due to such dilution of control advised to the personnel concerned.

13. Best Practices

13.1 The following are some of the best practices while guiding the IS Audit functions within the Bank.

a. Every bank to have an IS Audit Policy.

b. IS Audit should be a Risk based exercise.

c. The observations in the IS Audit report may have to be rectified in a time bound manner, say within 3 to 6 months from the date of completion of the IS Audit.

d. There needs to be a policy towards conducting the first audit of a newly computerized branch within a specific time frame E.g. within 2 months of the implementation. It can be called say "Take-on audit" etc.. Its coverage can be Access controls, Conversion controls and Contingency issues like Backup etc. Preferably, the take-on audit report could be closed within One month from the date of report.

e. The IS Audit report can rate the current status of the IT Security in the branch/office under review. The Risk at each site is to be assessed by the Inspection Department so that corrective steps can be taken for rectification and risk management. This is possible only if the branches/offices under review are graded based on the lines of the Regular Inspection system.

f. The IS Audit gradation may be linked to the Regular Inspection gradation. If any IT related fraud is found then the Gradation should be decided accordingly. Also it can be integrated with the Regular Inspection for conducting the audit and awarding gradations.

g. IS Audit may be done by an agency independent of the CPPD or the Implementing agency within the Bank. E.g. IS Audit Section as a part of the Inspection Department of the Bank. Security is as good as the last update. Therefore, IS audit should be done at predetermined intervals such as quarterly, half-yearly etc..

h. Also, updation of security policy of the Bank should be a continuous process. It should always be up to date which smoothens the process of introducing new technology products.

i. The IS Audit checklist may be clearly segregated on the following lines

1. Environmental controls
2. Logical access controls
3. Physical access controls
4. Procedural controls
5. Parametric controls
6. Implementation controls (Conversion etc.,)
7. Hardware/Software maintenance
8. DBA activities
9. Contingency plans (Business continuity, Backup, DRP etc.,)

13.2 Controls over the implementing agencies like CPPD through periodic IS Audit of the administrative offices in-charge of implementation for 'processes' can be included in the scope of policy document.

13.3 There could be a procedure for periodic Hardware Audit as a part of the regular IS Audit. This could check the configuration details of all the Hardware supplied for agreement with the Order copies.

13.4 Banks may have separate cells/sections for undertaking Research and development in Information Security and Systems audit.

14. Computer Aided Audit Techniques (CAAT)

14.1 CAATs are generic audit tools. They come with a lot of facilities including statistical and mathematical queries on database that holds client/management information. They work on many file formats.

14.2 They can be used by, general auditors with minimum IT background, but adequate aptitude after an initial training to assist them to take out queries relating to inspection/audit.

14.3 These tools work independent of the application package. They can assist inspectors/auditors in locating revenue leakages, identifying early warning signals such as potential NPAs, fraud prone areas etc.

14.4 Unlike audit modules that could be supplied by an application package vendor, CAATs have the advantage of working on any platform. This means, if the bank is migrating from one platform to another/one package to another, CAATs can still be re-used with minimum additional effort.

14.5 Moreover, if there is any change in the business rule, users have to normally rely on the application package vendor for changing the Audit module also. CAATs do not suffer from that disadvantage. They can be modified by trained end-users (inspectors in the case of inspection department) with minimum effort.

14.6 CAATs also do not alter the database, so could be used by beginners without fear of losing data integrity and controls. Though the queries, generated by CAATs could also be generated by query languages related to the RDBMS, such as SQL, wrong use of SQL could result in total loss of data and controls.

14.7 The CAAT's logic being independent of programming logic, they have the additional advantage of indirectly cross-verifying the veracity of underlying programming logic. CAATs can also be effectively used in branch/operational audit to verify the uniformity of parameterization, uniformity of customization and implementation at different branch locations.

15. Report Writing and Submission

15.1 After collection of relevant details through Checklists, Printouts and Audit Notes taken at the time of IS Audit the report has to be compiled in the specific format suggested. It should be addressed to the assigned authority and under instructions copies of the reports are to be submitted to the concerned branches/controlling authorities.

15.2 With regard to sensitive observations in Operations the report should be submitted in confidence to the assigned authority as a Special Report. Copies of such Special Reports should not be marked to the branches.

!5.3 With regard to weak controls observed in the Application Software the observations are to be listed out separately and sent to the assigned authority in confidence. Wherever the same Application Software is running, such weak controls will also be common. Hence it is a matter of urgency to report such weak controls immediately and in confidence. Copies of such confidential observations should not be marked to the branches.

15.4 The enhancements and modifications to the Application Software sought for by the branches are to be analyzed thoroughly and added as suggestions to the report.

15.5 The weak controls identified by the auditor should be categorized as "High, Medium and Low" so that high risk areas are addressed on a priority basis.

15.6 All audit reports must have specified time frames for comments and remedial action by the concerned auditee. It is suggested that security audit reports of large and sensitive systems like core banking applications, high value and volume transactions/ reconciliation systems like FOREX operations, Inter-branch reconciliation, ATM networks should be closed expeditiously, say within a month or such prescribed periodicity unless the corrective action involves software development or other prolonged measures.

15.7 The concern of the banks in managing computerized systems is to ensure uninterrupted business, prevention of computer frauds and increased benefits through computerization with manageable risks. IS Audit is an effective and specialized function which fulfils this requirement.

Operational Control

1. Introduction

1.1 Computer Operations relate to the implementation of the guidelines/rules and regulations relating to the business of the organization. While 'flexibility' is very important for smooth operations, 'security and controls' are vital to ensure reliability. Here are a few control aspects for successfully controlling the risks and vulnerabilities in the operational area of branch computerization.

a. Given below are some of the controls, which are desired to be practiced, and the implication statements describing what is in store if the controls are violated.

2. Preservation of Master Creation Documents/Conversion Controls

2.1 **Preventive Controls**

2.1.1 Whenever Applications under Manual Systems are switched over to Computer
Systems it is desirable to have the 'turn around documents' (printouts of data converted)
certified by the Officers and kept as permanent record of the branch.

E.g.: Final Printouts of Ledger details, list of balances etc., 2.1.2. The specimen cards will have to be converted into digital images using signature capture system. However, physical cards should be maintained for verification in case of need.

2.1.3 The opening forms, specimen cards etc., shall continue to be maintained as usual.

2.1.4 Ensure that Master Data Created (normally entrusted to outside agency when an existing manual branch is being computerized) is compulsorily verified and authorized by branch officials. If the master data is not authorized, the operator level users can modify it. Hence authorization of all master data will be a step towards prevention of frauds.

2.1.5 Conversion controls are preventive procedures to be observed while switching over from manual environment to computerized environment. Some of the important items to be taken care of are

a. All the heads of accounts should have been balanced and tallied before conversion.

b. The balancing before and after the conversion should tally.

c. Before the conversion, the branch head should authorize for proceeding for the conversion.

d. The conversion documents should be authorized and preserved.

e. The conversion should be done on the same day for all the accounts under a particular account/GL head.

f. Controls could be built over the DUMMY, ZERO Balance accounts.

Example: When the computerization is taken up for a branch and the conversion is being done from the Manual to TBC or ALPM to TBC, the day book balance is first updated to a DUMMY account which could be say SB/0 or CA/O. This is for the day book purposes. Once the process of opening all the accounts is complete in the new system, the balances are distributed across all the accounts and the SB/0 is made as Zero balance. This account has potential to be misused. This account should be closed under proper controls. Like wise the mismatches or standard differences are parked in certain mismatch accounts like account number 99999999 to satisfy the requirements of double entry book keeping in the application packages/databases. The balance lying in such accounts should be reconciled as early as possible. Until such time the account should not, be allowed to be operated by normal users. Any transaction arising in such accounts should be shown as 'exception' and should figure in special reports and should be available for scrutiny by auditors etc. Such transactions should be authorized preferably by a higher-level officer say Branch head under dual control.

2.2 Implication in not observing the control(s)

2.2.1 If such documents are not preserved under proper authentication, in case of a dispute at a later date regarding either fixed details or balances, the Bank will not have sufficient proof to defend or locate the error.

3. Preservation of Operational Floppies/Control Floppies

3.1 **Preventive Controls**

3.1.1 Computer Systems use either control floppies to boot the system or use log floppies. Some of the sensitive menus like modification to parameters etc., are given as installation/control/boot floppies. It is imperative to preserve these floppies under safe custody.

3.2 **Implication in not observing the control(s)**

3.2.1 If the floppies are not kept under proper control it may be misused for unauthorized access to the Computer systems.

3.2.2 Loss of such floppies will also result in delay in booting the systems and business interruption.

4. Training

4.1 **Preventive Controls**

4.1.1 Proper training for various Computer Personnel like Operators, Supervisors, System Administrators is a prerequisite for efficient operations.

4.1.2 The training is to be designed according to varying needs, functionalities and job roles.

4.1.3 On the job training for the second line personnel especially in 'System Administration' is a must.

4.2 **Implication in not observing the control(s)**

4.2.1 In a live environment 'Data' is a very valuable thing. If a Computerized system falls into untrained hands, loss or corruption of data is a possibility. Reconstruction of Data and ensuring 'Data Integrity' is a time consuming and painful job if tried through untrained personnel.

5. Maintenance of Registers

5.1 **Preventive Controls**

5.1.1 Control Registers give the events in chronological order and hence forms the best part of Internal Control mechanism. The various suggested registers are

a. Register of Computer Inventory

b. Register of Stocks, fresh floppies, tapes, and stationery

c. Register of System Managers/Data base administrators along with their IDs

d. Register of Errors and Breakdowns

e. Register of Insurance

f. Register of Annual Maintenance Contract

g. Register of Outputs (Printouts)

h. Register of Backups (CTDs/DATs/Floppies)

i. Register of Off-site Storage of Backups

j. Register of authorized users

k. Register of deleted users.

1. Register of details of the vendors, electrical Engineers along with their phone numbers.

m. Register of User-ids of all the persons introduced to the system from the beginning along with the other details like when they were introduced to the system and status - active/inactive and the reasons for the same. This will be signed by the employees against their respective Ids in token of accepting their responsibilities against that user ID.

n. System access register should be maintained to record the details of the persons who entered the system room. This should contain details like name of the person, purpose of visit, time in and time out.

o. Key register - A record of keys to the system room including inner receptacles and their usage by various personnel.

5.2 **Implication in not observing the control(s)**

5.2.1 Non-Maintenance of prescribed registers will lead to searching for information from various files/records and such collected information will be inconsistent from time to time.

5.2.2 Registers and the entries give a clear understanding for the future users of the systems and are very effective whenever person’s change and handing over/ taking over take place. This purpose will be lost if the registers are not maintained.

5.2.3 The registers are good indicators of vendors/system performance. If the errors and breakdown registers/vendor call registers are not maintained properly the above feedback will be lost.

6. Application Software Passwords/User-IDs/User Levels

6.1 **Preventive Controls**

6.1.1 An important access control mechanism available through software is the 'Password mechanism'. Passwords are normally encrypted and are known only to the users. In highly critical and sensitive financial systems it would be advisable to create passwords for the users, in parts, by different security officers (User control Officers). Maintaining the confidentiality of passwords is the first and foremost preventive control.

6.1.2 Effective Password mechanism allows the user to change the Password on his/her own periodically. Sometimes the System forces the user to change the password after 'stale time'.

6.1.3 Passwords should have a minimum length of say 5 to 6 characters alphanumeric and it should not be easily guessable/decipherable.

6.1.4 Passwords should be uniquely linked to User-IDs (User Identification).

6.1.5 Th^e transactions should be tagged with the respective user's User-ID. This is to ensure, while perusing a transaction one must be able to identify as to who has raised the transaction, who has authorized the transaction/passed the transaction.

6.1.6 User-ID and Password should not be the same.

6.1.7 The system should have the capability to trap the terminal-ID from where the user has put through the transaction.

6.1.8 Provision for classifying User-IDs as "read only", "read/write", etc.. maybe available in the system.

6.1.9 Apart from the Passwords and User-IDs, the system should provide Level numbers for different users. Viz., System Manager, Chief Manager, Senior Manager, Manager, Asst Manager, Clerk, Shroff, Chief Cashiers etc.,

6.1.10 Depending on this 'User level' persons derive powers for passing, authorizing and doing any other special functions.

6.1.11 Administration of such User-IDs/User Levels may vest with the System Administrator or under dual control.

6.1.12 User Creation and Deletion: Users should be created only after authorization from a designated branch official. This pertains to the users at the system level (OS/RDBMS) or at the application level. This is an important area for effective IT Vigilance in computerized branches.

6.1.13 A register to record and authorize all users created in the system could be maintained and kept under custody of a senior functionary of the branch. It could contain the signatures of the user, System administrator, Branch Manager for creation and deletion with roles and privileges granted to a user, date of creation/deletion etc..

6.1.14 Creating, activating, deactivating and deleting User-IDs/User Levels are sensitive functions and hence should be done under dual electronic authorizations.

6.1.15 Review of extraneous users should be made periodically by a person oilier than the system administrator and recorded by the branch. Such users should be deleted and all transactions that have taken place under that User-ID from the date of last review/creation of the User-ID should be scrutinized to know the genuineness of such transactions/activity.

6.1.16 Automatic deletion of user profiles if not used for more than say 3 days could be a feature of branch application software. This can dramatically reduce the chances of any misuse by branch users.

6.1.17 The Password of an ‘active user' should be known only to the user and has to be kept secret by him.

6.1.18 At times the role of a System Administrator/OS Supervisor may have to be played by another person in the absence of the designated person. To meet such exigencies, alternate arrangement for smooth change over has to be made. One of the suggested methods is that the Supervisor/Sys Admin Password has to be kept in a sealed cover with a higher authority.

6.1.19 No user should disclose his password to others at any point of time. Likewise no user should use other's passwords under any circumstance. Likewise users of lower level should not use higher-level functions for passing beyond prescribed powers/authority. Likewise, Operators (Clerks) using Officers' Password, Clerks acting as System Administrators, Asst Managers and Managers using Chief Manager's Password for authorizing etc., should be totally avoided.

6.1.20 Hence wherever the Password discipline is violated the Branch Manager and the System Administrator are to be appraised for immediate corrective action.

6.1.21 Additional precautions

a. No generic User IDs to any user without reflecting the actual names

b. Password could be alphanumeric

c. No user to exist without any password (System controlled)

d. What cannot be a password (passwords reflecting one's personality etc.,)

e. Not to be written anywhere

f. Password could be changed only by the respective users. The system should prompt the user to enter the previously used password when the system prompts
for a password change. Unique password feature (disallow use of old password) should be enabled after say 6 to 12 rounds.

g. Access may be controlled for non-offices hours/Days reasonably.
h. Storing of passwords in function keys could be deactivated.

i. Vendor may not be provided with a dedicated profile in system.

j. The system should provide the users the capability to disable their user-ids when they proceed on leave and should be enabled only by the system administrator and with the consent of the user.

k. Users created for audit/maintenance purpose are disabled immediately after the work is done.

1. Intruder lock out should be introduced in the system to prevent unauthorized persons from trying to access the system by trial and error method. The maximum attempts should be kept to 3. After that the user will be locked out. The System Administrator will reintroduce him to system. The system should produce a log of failed attempts to log in, for further investigation.

6.2 The Passwords are case sensitive and hence stored/verified by the system exactly the way they are typed, e.g., the following are four different passwords and are not the same.

6.3 Some of the Do's and Don'ts for usage of Passwords are

6.3.1 Don'ts

- Do not use your first or last name
- Do not use your spouse's name
- Do not use other information easily obtained about you. This includes license plate numbers, telephone numbers, social security numbers, the brand of your automobile, the street names etc.

- Do not use a word contained in English Dictionary, spelling lists or other listed words

6.3.2 Do's

- Use a password with mixed-case alphabets
- Use a password with non-alphanumeric characters like punctuation mark
- Use a password that is easy to remember, so you don't have to write down
- Use a password that you can type quickly using keys on both sides of the key board so that the casual observers will not be able to easily guess.

6.4 Implication in not observing the control(s)

6.4.1 Absence of Password Controls, Misuse of Passwords, Absence of secrecy of Passwords will all lead to unauthorized transactions and problems for fixing identification/accountability. Dilution of such controls may lead to Computer Frauds.

6.4.2 Creating and deleting users without proper authorization from a designated official/under dual control will lead to unauthorized/extraneous users getting into the system and the transactions taking place in the system will lose their identity.

7. System Level Passwords/Login Controls

7.1 **Preventive Controls**

7.1.1 Apart from the Password Controls provided by the Application software, the Operating System provides boot-in password and System Login-ID in a Networking environment.

7.1.2 Each authorized user must be given a unique System Login-ID for proper identification of Login to the system.

7.1.3 The privileges given to various users at system level has to be carefully planned, implemented and monitored. It should be on 'need base'. May be at the time of installation of the system this can be controlled through a batch file so that the implementation across branches will be uniform. These privileges determine the rights for users to scan, read, write, delete, execute etc., The controls over the usage of such rights may be monitored to find out any abuse. Proper logs may be created and monitored to have effective control over this aspect.

7.1.4 DBA could have access to the O/S or RDBMS through his own ID. The generic powerful privileged users could be used only if the privileges given to the DBA user profile are not adequate. This considerably reduces the usage of privileged users profile to bare minimum.

7.1.5 Default passwords of sensitive user ids sent by the software vendor should be changed.

7.1.6 Remote access

a. Controls over the remote access to the application and system to customers or System Admin respectively should be adequate.

E.g.: the customer should be restricted from access to privy information in the system

b. Further, the remote troubleshooter should be restricted from accessing the system freely. The telephone number, which is permitted to access the system, should be controlled. E.g. one should not be able to access the branch database from an Internet cafe or home PC.

7.2 Implication in not observing the control(s)

7.2.1 In a integrated total computerized environment identification of each transaction such as who has created, who has modified, who has deleted and at what time of the day is a banking/audit requirement. If such identification is not made available as a system forced control, it may lead to dilution of controls and high risks.

7.2.2 If the users are given more privileges/rights than required it may lead to unintended access to directories and files, which the user is not entitled to. This may lead to a conflict of identity at a later time and users at different levels will feel insecure.

8. Authentication of Printouts/Exceptional Reports

8.1 Preventive Controls

8.1.1 Apart from the data available in the Magnetic Media it is an audit/legal requirement to generate, authenticate and preserve Printouts such as Daily Cash, Clearing, Transfer Scrolls, Sectional Day Books/Transaction Logs, Day Book, Statement of Account (Ledger Copies), Weekly/Monthly Balance Reports, GL/SUB GL Balances Report, A and L, P and L RBI Sec.(42), CA/CC/OD and Loans Products Report and other control reports. This requirement is also to satisfy the 'Bankers' Book of Evidence Act'. Alternatively, the Data output in magnetic media with suitable digital signature verification may also be preserved to satisfy any modification to provisions of 'Bankers' Book of Evidence Act'.

8.1.2 Exceptional Reports reveal all transactions where authorizations are required like excess/TODs given, cheque authorizations and oilier extraordinary transactions. Hence the Branch Manager or any other designated officer should peruse the report daily and satisfy himself that only authorized transactions have been put through the system and authenticate the report.

8.1.3 Such Exceptional transaction reports are to be preserved separately for perusal of auditors/inspecting officials.

8.1.4 Review of reports should be done periodically and exceptions handled appropriately.

8.1.5 Direct debits to GL a/cs should be controlled and monitored as exceptional transactions. E.g.: Direct debit to GL - Bills Purchased without routing through respective Sub-GLs and crediting the amount to individual accounts.

8.2 Implication in not observing the control(s)

i. If the computer printouts representing the transactions are kept without Officer's authentication then it will be difficult to identify genuine transactions from others in case of scrutiny at a later date and such unauthenticated printouts will not stand good evidence.

9. Daily Balances Report/Fall Back Report

9.1 **Preventive Controls**

9.1.1 Computer systems are prone to occasional breakdowns. Until the system is restarted the business has to be continued. For continuing the business, the branch may have to switch over to manual processing temporarily. The daily balances report of the previous day or Fall Back Reports will be used in such exigencies. Hence Branch should compulsorily generate such Fall Back reports/Daily Balances report before Day-End and preserve them as magnetic files in the Hard disk of the Supervisory Node and relevant printouts can be generated when required.

9.2 **Implication in not observing the control(s)**

9.2.1 If such fall back reports are not generated/printed out and preserved, the branch has to wait till the vendors arrive and set right the computer systems. This will lead to disruption of customer service and at times the back office functions such as servicing clearing returns will also suffer.

9.2.2 Also after restoration of computer systems once the data is restored the bank may need a check point from where the restart may take place. The fall back reports provide excellent checkpoints to confirm the data integrity.

10. Transaction Processing/Checking of consistency of Account Balances/Checking of Daily Transaction reports with vouchers

10.1 **Preventive Controls**

10.1.1 Printing of voluminous reports and storing them is not a good business practice. However, printing and storing of essential reports are required.

10.1.2 Each report should contain End of report marker along with the designation of the authority whose scrutiny is required for the report so that relevant reports can easily be handed over to the officials concerned.

10.1.3 Every transaction in a computerized environment, should be supported by a voucher either manually prepared or computer generated. At the time of transaction raising wherever the transaction number is automatically generated by the system, the number (batch no./node no./serial no.) may be written on the voucher and counter foil for easy identification.

10.1.4 Systems where printed documents are used for payments and other actions with financial implications, it should be ensured that such reports are printed by the system only once to prevent any duplicate payments. Once the printout is generated, the data/message should be parked/flagged and kept in the output message history. In case the original printout is damaged etc., the subsequent printout may be allowed by the system with a notification on the printout as 'Duplicate'.

10.1.5 In such application systems, where the master balance is displayed in the transaction screen/balance reports and the statement of account is generated from history files, one of the checks on Data Integrity (data consistency) is the checking of Master balance of an SB or CA with that of the balance generated in the Statement of Account option. These two should tally for a given account for a given date.

10.1.6 Raising a transaction and passing of the transaction should be vested with two different users, i.e. same user should not be allowed to raise and pass the transaction also. Normally the software will force such a control. If not, manual control should be exercised. This will introduce effectively the dual control.

10.1.7 Likewise Staff members should not raise or pass a transaction relating to their own or related accounts.

10.1.8 In-operative/dormant accounts should not be allowed to be operated as a matter of routine like any other accounts. All operations in such accounts have to be authorized by respective officials (say Branch-in-charge) before allowing operations.

10.1.9 There should be a provision to print the position of Dormant/Inoperative accounts to keep a watch on the operations of the account even after they become live. Sudden huge credits coming to these accounts should be investigated.

10.1.10 In a Totally and partially computerized environment the transactions are passed then and there with the vouchers and electronic authentications also take place. However it is highly desirable to check the day's vouchers with the Sectional Day Book or Scrolls or transaction Log. The checking officer should be other than the one who originally authenticated the voucher/transaction.

10.2 The Benefits are

10.2.1 Transactions passed erroneously during the busy hours of the day will get detected/corrected.

10.2.2 Duplication mistakes will get detected.

10.2.3 Wrong account classifications due to bad figures will get detected.

10.2.4 Some of the system generated transactions and passed automatically by the system get reviewed for their correctness.

10.2.5 Any unauthorized transaction put through the system without vouchers will get detected.

10.2.6 It will be a deterrent against frauds/misappropriation.

10.2.7 Any missing voucher gets detected.

10.3 Implication in not observing the control(s)

10.3.1 If such a system of post-checking of vouchers is absent it can be exploited by someone for commission of frauds.

10.3.2 Any error due to compensatory mistakes will go undetected.

10.3.3 All missing vouchers/transactions conducted without supporting vouchers are to be brought to the notice of the branch-in-charge/systems manager for verification of the genuineness of such transactions.

11. Backups and Contingency Planning

11.1 Permanent Backups/Software Backups

11.1.1 It is desirable to take copies of latest version of Application Software and preserve them as permanent Backups. The Backups may be taken in floppies or Cartridge Tapes. Such Backups will be used for restoration in case of disk crash etc., If Backups of System Floppies are possible they may also be preserved separately.

11.1.2 Take fresh backup of application software whenever version changes happen. That is, a copy of latest version of the application software should be held as backup for recovery in case of failure.

11.1.3 In case of ZIP drives the chances of failure are remote.

11.2 Permanent Back up of Data

11.2.1 Backups of Data files used for creation of Master files during switch over to computerization are to be preserved as permanent backups either in tapes or floppies.

11.2.2 Backups of data files of important days like Interest posting days, Quarterly, Half Yearly, Yearly closing days, Days on which software/data structures are changed and days when troubleshooting due to data corruption/index corruption are undertaken, should be preserved for later diagnosis/use.

11.3 Floating Backup/Daily Backup of Data

11.3.1 At the end of each day before commencement of 'Day-End' procedure it is mandatory to take a backup of all data files. Some systems force the user to take backups and some do not. Hence whether it be a system generated control or manual control Day Backup is to be taken and preserved.

11.3.2 Such backups of consecutive days in separate tapes/floppies are preserved as 'Grandfather, Father, Son' Backups. It is desirable to have a cycle of one week for rotation of the backups. In case during start of the day, the system crashes the backup of previous day could be used for restoration of data. If due to some reason the backup is unusable due to media failure etc., then the preceding day's backup can be used. Thus having six previous days' backup will help restoration from a desired date.

11.3.3 Care should be taken to take consecutive day's backup in separate tapes/floppies. This is to ensure that backup of 2 or 3 days data is not lost due to media failure.

11.3.4 The on-site backup media has to be stored and preserved in a Fire proof Cabinet inside the computerized branch under dual custody. If possible another copy of the data backup media may be kept inside the strong room in a locker for additional safety. This will protect the backups in case of burglary/Fire etc.

11.3.5 The daily back ups can be as follows:

a. Backup of data from live area to hard disk before doing end of day.

b. Before end of day to be taken on another volume of the file server.

c. After end of day back-up to be taken in yet another volume of the file server.

d. Tape Cartridge/CTD backup: Separate tapes shall be used for each day of the
week.

11.4 Additional Precautions

11.4.1 Types of Backup, which needs to be taken, should be decided by the banks depending on the type of database used and should be specified explicitly to the users. E.g. Full tape backup, Online archival, Daily Contingency backup with basic data etc.

11.4.2 Contents of the daily backup is to be specified in the bank's procedure. E.g. All data files, Controls files, redo log files, password file etc., or else there will be If incomplete backup. UNIX backup is a junk in case of incomplete backup (incomplete files).

11.5 Purging and Retrieval

11.5.1 One of the important periodical routines is the purging of the old and not-immediately-required data to the archive tapes/media. While doing so the following items may be taken care of.

11.5.2 The size of the data available in branches should be manageable, compact and sequentially arranged for retrieving it for specific requirements. As such the data relating to a certain period may be purged and archived. There should be a system of Archiving the old/historical data on CDs and may be preserved as an off-site backup also.

a. Fully reconciled heads only to be purged.

b. Purged data should be retained for at least a minimum number of years, say, 8
years depending on the old record policy of the bank and legal requirements.

c. The purged data should be retrievable at any point of time during these 8 years
with data integrity.

11.6 Off-site backups

11.6.1 One copy of the Permanent/Floating Backups are to be kept in another location, say another branch/bank, under safe custody.

11.6.2 Necessary Precaution has to be taken to ensure that such Backups are handed over/taken over under due authentication/authority.

11.6.3 Such backups should not be allowed to fall into unauthorized hands.

11.6.4 Th^{e} tape back up is to be tested for retrieval otherwise the very purpose of such backup is defeated when the data is to be restored.

11.6.5 Proper records should be maintained for the tapes maintained at the off-site location, with information such as tape number, date of backup, contents, recycle date, etc..

11.7 **Milestone backups**

11.7.1 Milestone backups (Annual Backup etc.,) should be cut into CDs at controlling offices and a copy of the same may be preserved in the branches and one at the controlling office.

11.8 Implication in not observing the control(s)

11.8.1 Absence of proper Backups will lead to bad contingency planning.

11.8.2 It will lead to manually re-entering the data from the last available backup date, which will take enormous time and effort.

11.8.3 Even after such an exercise, the Integrity (Correctness and Accuracy) of data has to be tested thoroughly resulting in further delay and anxiety.

11.8.4 Keeping the Backups in the same premises will lead to destruction of originals as well as Backups in case of Fire, Flood, Burglary etc., Hence the importance of Off-site Backups.

12. Software Modifications/Version Changes

12.1 **Preventive Controls**

12.1.1 Application software is prone to modifications for fixing of Software Bugs/Enhancements. It is desirable to record such visits of vendors and details of modifications carried out in a register.

12.1.2 While allowing the vendor to port new versions of software/copying of files, Backup of the old version is to be taken in a Media/tape and preserved before handing over the system to the vendors.

12.1.3 Preferably the data backup may also be taken. It should be ensured that the vendor's representative has the requisite authority from the Bank for carrying out the modifications.

12.1.4 Adequate controls should be exercised over Ad-hoc/Patch programs, which are written by the Implementing officers for trouble shooting or MIS purposes.

12.2 **Implication in not observing the control(s)**

12.2.1 Absence of proper preventive control as above will lead to unauthorized modifications to the software and may lead to data integrity problems-computer frauds.

12.2.2 Change of versions/version controls cannot be monitored and uniformity across the branches cannot be maintained.

13. Economy in Expenditure

13.1 **Preventive Controls**

13.1.1 In a Computer Environment, considerable expenditure is involved in the purchase and use of consumables like Computer Stationery, Floppies, Cartridge

Tapes and Printer ribbon refills etc.. It is desirable to maintain proper control over such consumption.

13.1.2 Printing of reports may be centralized to a great extent possible to avoid duplication of printing and to avoid wastage of stationery.

13.2 **Implication in not observing the control(s)**

13.2.1 The purpose of computerization should be to avoid wasteful expenditure - economies on cost of operations and to move towards paper less banking in the long run. Hence it is essential to look into the practices in a computerized environment and change the mindset-lest cost of operations/saving measures will receive a set back.

14. Preservation of Printouts

14.1 **Preventive Controls**

14.1.1 Considerable effort is put up for taking printouts in a computer environment. Since different kinds of reports can be generated using same data there is redundancy in generation of the same information. Hence it is very important to optimize on what needs to be printed and preserved.

14.1.2 All printouts are to be bound, labeled, disclosing the period, its serial number and arranged in an organized manner and a Register of such volumes is to be maintained for easy retrieval.

14.2 **Implication in not observing the control(s)s**

14.2.1 If printouts are not preserved properly, considerable time will be wasted in searching for information leading to frustration and sometimes delay in house keeping/customer service/audit/investigations etc.

15. Access to Operating System

15.1 **Preventive Controls**

15.1.1 The Application software used in computerized branches should facilitate direct access to menus when logged-on and on exit should not allow access to operating system prompt nor any rights for the user to delete the files directly from the OS prompt.

15.1.2 Controls could be built over the access to Operating system software through control key combinations. E.g. Inclusion of TRAP command in the DOT profiles

15.2 **Implication in not observing the control(s)**

15.2.1 If access to OS is not restricted, it will result in accidental/intentional deletion of files by the users.

15.2.2 Usage of Operating system commands by unauthorized persons resulting in unauthorized modifications, deletions and loss of data/programs.

15.2.3 Unauthorized usage of OS may result in users running extraneous programs outside the purview of the application software leading to unethical practices.

16. Usage of Unauthorized Programs/Computer Virus/Misuse

16.1 **Preventive Controls**

16.1.1 Computerized branches supplied with Application Software should use only authorized/licensed programs in the Computer Systems.

16.1.2 Usage of unauthorized software, extraneous programs, Games software and usage of unauthorized 'guest floppies' should be totally prohibited.

16.2 Implication in not observing the control(s)

16.2.1 Usage of Unauthorized programs/Games floppies/'Guest Floppies' will result in valuable disk space getting occupied leaving the authorized programs suffering.

16.2.2 'Computer Virus' is another danger caused by such 'guest floppies'.

16.2.3 The work discipline will get diluted resulting in misuse of 'Computer Time' and computer resources.

17. Management of Computer Resources/Job Rotation

17.1 **Preventive Controls**

17.1.1 Computer resources such as Hardware, Software, 'Computer Time' are to be managed by well trained personnel. Though considerable effort is put up by the Corporate offices of Banks to impart theoretical/practical training, there is no replacement to 'gained experience' through systematic on the job training, in a Computer environment. Hence it is imperative to place the management of computer resources in the hands of personnel with good aptitude to learning and teaching others. The experience gained on the Application software has to be imparted to others to ensure continuity of operations.

17.1.2 Job rotation is another control to ensure spreading the familiarity of operations among various personnel for smooth customer service. Also it will be a deterrent against Computer Frauds.

17.1.3 Job cards/application run charts should be given to operating staff for reference and compliance with guidelines.

17.1.4 Alternate Officers should be necessarily trained on System Administration functions by allowing them to do a whole day's job of the System Administrator, every now and then. This will enable smooth change over of Computer Management in case the designated SA goes on leave, transfer etc.,

17.1.5 When an employee from one dept/cell is transferred to other dept/cell on rotation, care should be taken to change his access rights so as to prevent him from accessing the menus of the old dept/cell. Similarly when employees proceed on leave, their User-IDs should be temporarily disabled; when employees are transferred out of the branch/office, their user-ids should be deleted.

17.2 **Implication in not observing the control(s)**

17.2.1 Lack of Job rotation and developing second line on specialized areas such as System administration will create indispensability in key areas of operations. This will create a vacuum in talent in a computerized branch when the only trained person leaves the branch on transfer etc.,

17.2.2 Business continuity/computer operations will suffer.

17.2.3 It will raise doubts on the system integrity and the auditability of systems will suffer.

17.2.4 Too much dependence on one person will lead to operational rigidity leading to friction in work environment.

18. Leakage of Income

18.1 Preventive Controls

18.1.1 Leakage of Income occurs mainly in application of interest in CA/CC/OD/Loan accounts and charging of interest in Bills related transactions. Interest rates are fed into parameter files, account wise or GL type wise for a period range. Correct interest rates (Normal Rate and Penal Rate) are to be fed to the parameter file. As and when changes to rates of interest are informed it should be immediately fed to the computer, at least before the quarter end.

18.1.2 If interest calculation is not taken care of retrospectively (i.e. from effective date) then necessary manual adjustments are to be made to recover the interest due.

18.1.3 Before application of interest on the last day of the quarter, thorough check of the Interest rates fed to various accounts are to be done to ensure that only correct rates are fed in the parameter file.

18.1.4 At the end of the quarter, after application of interest a sample check of a few large borrowal accounts are to be done to ensure that the interest amounts debited to the accounts by the system are correct.

18.1.5 Like wise, the service charges and other charges automatically raised by the system are to be test checked for accuracy-leakage of Income.

18.1.6 Like wise the interest paid on deposit accounts have to be test checked to prevent excess payments.

18.1.7 Control over the "Interest/Commission Credit accounts" (the account where the contra credit for all the interest debits posted to the Advance accounts is credited through an application as and when the interest is applied) should be adequately exercised. This can have dramatic impact on preventive vigilance.

18.1.8 Once the quarterly/half yearly interest is applied the balance in the interest account should be initialized. A report may be generated of interest provided a/c with the nil balance and this should be checked by appropriate authority.

18.1.9 The changes to interest rates and Limits should be carried out only by an authorized official. There should be a limit/interest change register to record such changes. All such changes which fall in the category of non-financial inputs to the system (but have financial implications eventually) should be duly authorized by an appropriate supervisor on a specially designed non-financial input form.

18.1.10 Interest rate adjustments, changes and other parameter settings like staff accounts, codes for concessional interest rates should be given by the system in the form of a control report. This should be scrutinized independently by an official other than the person who has authorized preferably, by the Concurrent Auditor in large branches.

18.2 Implication in not observing the control(s)

18.2.1 Lack of verification of interest charged/service charges calculated by the system will lead to leakage of income and the cumulative effect of all such branches will be enormous and will in turn affect the profitability of the banks.

18.2.2 Lack of periodical verification of income leakage will lead to income leakage pattern which will have spiraling effect on the system.

19. Book Adjustment/House Keeping

19.1 Preventive Controls

19.1.1 One of the major benefits of computerization is balancing of books and automatic generation of ledger balances. Desired number of copies can also be generated. Also balances can be generated for a 'given date'. Using this to the advantage computerized branches should try to match the total of account balances with the Sub GL/General Ledger Balances.

19.1.2 Also, verification of sum of Sub GL balances with the GL balance is to be done. The total of Sub GLs should be correctly reflected as consolidated GL figure. Apart from the above the nominal accounts such as Bankers Payment Order, Sundry Deposits/Suspense accounts, Receivable A/Cs, Margins on Bills purchased and Guarantees are kept as separate registers in the computer system. These register balances are to be tallied with the control figures available in relevant GL/Sub GLs.

19.1.3 At the time of computerization as on a cut-off date the books are to be balanced/adjusted and only such adjusted figures incorporated in the computerized systems. But due to practical difficulties there is a time lag between the date of computerization and the date when the account balances get reconciled. In such cases the difference is kept in 'difference account' in certain cases and as and when differences are located the account gets wiped off. Details of such account details are to be analyzed to ensure book adjustment and data integrity.

19.1.4 After tallying the entries in the 'difference account', such accounts should be closed or frozen to prevent any unauthorized transaction subsequently in such accounts.

19.1.5 It should not be assumed that computerization will automatically take care of book adjustment/balancing of books. Even after computerization, branches should generate balances every month/periodically to ensure that the ledger/register balances tally with relevant Sub GLs/GLs. Such control figures should be recorded in a register and authenticated by Officers assigned. This is a preventive control against any unauthorized change to magnetic data files retrospectively.

19.2 Implication in not observing the control(s)

19.2.1 If the computer operations are not reviewed by the branches with regard to Book Adjustment/House keeping periodically, it will result in loss of data integrity. Software Bugs, Program errors will go undetected resulting in excess/short payments of interest/credits/debits and other errors.

19.2.2 Verification of SB-TODs at the time of balancing of books is a must. The TODs may arise due to System generated compulsory debits (such as Clearing Inward Returns/Service Charges/Automatic debiting of Interest etc.,) or due to authorizations directly in the computer with or without Funds book. Hence SB-TOD/CA-TOD reports are to be periodically generated to have control over such balances. Early adjustment of the TODs and analysis to prevent such TODs are to be done. Care should be taken to detect/prevent "concealed TODs" by carefully examining exceptional transaction reports etc.,

19.2.3 Book adjustment/balancing also ensure that all the credits/debits, which have come into the banking system, are properly accounted for and the respective accounts are credited/debited. If such checkpoints are not ensured, this will lead to customer dissatisfaction.

20. Physical Security/Preventive Measures

20.1 **Preventive Controls**

20.1.1 To prevent burglary

a. Rolling shutters are to be provided by the branches if not already in place, with
central locking system for the main entrance.

b. Window grills to have additional guard bars.

c. Glass doors to have grills.

d. Incorporation of additional security measures like installation of passive infrared
intruder alarm system and stand alone siren with the existing burglar alarm system.

e. Provision of security lights.

f. Local Police may be requested to intensify night patrolling in the area.

20.1.2 Adequate Fire extinguishers should be provided.

20.1.3 Appropriate Insurance policies such as Storage-cum-Erection policy, Electronic Equipment Policy and Fire Policy with relevant clauses covering risks arising out of Burglary, Theft, Fire, Riots, Earthquakes and others relating to physical loss of computer systems should be taken and kept in force always as per guidelines.

20.1.4 During start of the day and before closing the branch it is a desirable practice to check whether Computer systems are safe and secure and they are adequately protected.

20.1.5 At the end of the day it should be ensured that the Converter (Input) of the UPS is kept 'ON' and the Inverter (Output) of the UPS is kept 'OFF. This will enable the batteries to get charged overnight and avoid wastage of 'out put' power respectively.

20.1.6 Normally it is the practice in branches, that the System Manager has to sit late and he is the only officer available in the branch in late hours. As a security measure, the branch-in-charge or the second-line officer should be available with the System Manager till that day's jobs are completed and the systems are shut down.

20.1.7 Posting of a guard may be considered, if cost effective

20.2 Implication in not observing the control(s)

20.2.1 To find immediate replacement for the computer systems lost may prove difficult.

20.2.2 If the Server/Supervisory Workstations are burgled, there is immediate loss of primary data, software, Operating systems etc.,

20.2.3 Loss of data may result in loss of confidentiality of information.

20.2.4 Reinstalling the server/Main computer/Host, data reloading, testing the integrity of the software/data will become time consuming.

20.2.5 Possible business disruption.

20.2.6 Lack of timely and immediate vendor support and their co-ordination.

20.2.7 Lack of effective Crisis Management.

20.2.8 Hardships to be faced in lodging complaints with the police, insurance company, evidence collection, follow-up of claims etc.,

20.2.9 Possible loss of image for the bank/branch and possible adverse publicity

20.2.10 Anxiety of the customers about safety/accuracy of information.

21. System Administration Functions

21.1 Total branch computerization effectively introduces a multi-user environment and there is therefore, a need to oversee constantly certain vital and sensitive parameters by an authorized and knowledgeable person (called System Administrator) with clearly defined lines of responsibility.

21.2 The System Administrator will also act as 'Netware Supervisor' in case of TBC-LAN environment. Additionally he will be monitoring the OS functions.

21.3 Some of the System Admin functions which are specific to the TBC/PBC under LAN environment are given below:

21.3.1 Procedural/Software Guidelines/Controls with regard to the following areas are to be strictly adhered to

1. Branch Parameters/Drawing Power, Interest Rate parameters, Deposit Rate Parameters etc.,
2. User Creation, Activation, Deactivation (In case of leave etc.,) Deletion (On transfer etc.,) Terminal Assignment.
3. Separate User IDs/Levels, Prescribed Financial/Authorization Powers and Administration of Passwords.
4. Menu Access rights and Restricted Access parameters.
5. Holiday Master Maintenance.
6. Begin Day/End Day Procedures.
7. Backup Procedures, Periodicity for Preservation of Backups, Off-site Backups and Contingency Planning.
8. Locking up of Master Files for prevention of unauthorized changes. E.g: GL/SUBGL, SB/CA-CC-OD Balances Locking

9. Overseeing of performance of Computer Systems, Co-ordination with vendors etc.,

10. Co-ordination with other staff members for proper housekeeping and data integrity.

11. Hard Disk Space management, System Performance Review etc.,

12. Training of Second Line for System administrator.

13. Signature Scanning, remote servicing, Inter-connectivity of branches etc..

14. 'Netware Supervisor/Admin' Functions and responsibilities.

15. Supervision over Fully Mirrored Status of Hard Disks/Servers, Redundancy of Power (UPS), Servers and uninterrupted Computer Functions.

16. Creation of 'Alternate Netware Supervisor' 'Alternate Application System Administrator'.

17. Password administration, Maintenance of Secrecy of Password, Keeping Password of Sys Admin/Supervisor/Alternates under sealed cover/safe custody.

18. Restricted access to Server Console and Server Room for prevention of Unauthorized access.

19. Monitoring of Disk Performance such as Mirroring, Redirected Blocks, Down time, Data Safety

20. Restriction of usage of External floppies, Games floppies etc.,

21. Enabling and Disabling Login and restricted access to Application menus as per guidelines.

22. Disabling provisions of access to Operating System by users.

23. Generation of control reports and reports generated centrally.

24. Monitoring of Change of Passwords by users.

25. Monitoring of Difference Accounts maintained in computers after locking of balances.

26. Periodical Purging of old data and proper preservation of history data files.

27. Maintenance of all original software floppies, system floppies, original manuals, Software License agreements etc.,

28. Proper consistency checks provided through Software and Manual controls to ensure data safety and data integrity.

29. Monitoring of System controls to arrest Income Leakage.

30. Liaison with Software Vendors, EDPs, CPPD for improvement to the Application Software, Plugging of Security Lapses noticed in the Software, Exercising alternate Manual controls to arrest weak controls in the Software until they are rectified.

31. Latest Version of Software is ported and Changes to Application Software by vendors are monitored for its authenticity.

32. Controls over the data that is sent/uploaded through floppies should be exercised.

21.4 In a totally computerized branch, too often, computer security issues emerge due to lack of proper understanding of the operational controls by the users. The desired controls enumerated above and the implication statements will present a good clarity to all the users. If these controls are followed meticulously the vulnerabilities and risks will be reduced to the minimum.

Application Software Control

1. Introduction

1.1 The application software for computerized branches take care of computer security through in built features. It is essential to take care of critical security controls through system forced controls than leaving it to the discretion of users or to the manual controls. Some of the best practices in administering such controls through application software are given below as a matter of prevention against data integrity loss and frauds through manipulation of computerized databases.

2. Security Features

2.1 The various desirable security features include

a. User type, level and access rights

b. Access to Menus, database and system prompt

c. Security features in Transaction processing

d. Security to protect Master files

d. Security features specific to various application modules

3. User Types, User Levels, Menus and Access Rights

3.1 Different users of the application software may be classified according to their hierarchy, financial powers and authorization powers. Through extensive parameterization the users can be grouped to have uniform rights with facility to de-link a particular user from a specified right.

3.2 The System Administrator/Data Base administrator may be given a set of access rights. The Menus may relate to controlling the functions/powers/vital parameters, levels of other users.

3.3 All other Users may be given rights of access relating to Transaction Processing and their powers may be restricted according to their hierarchy and as per guidelines of the Bank with a proper relation to Manual environment.

3.4 System Manager may not be allowed to access Transaction Menus and other users may not be allowed to have access to System Admin Menu.

3.5 Even within each Level there may be sub-levels based on limits of access.

3.6 Unique sets of Restricted Menus may be related to each of the above level numbers. Thus a User with a given Level Number can have access to only predefined Menus fixed for them.

3.7 This security feature should deny access to Users to other Menus unrelated to them thus protecting various Files.

3.8 Following application and IT Controls may be built into all the applications to ensure the following

a. **Completeness and accuracy of inputs**

The input forms should contain all the information that are to be fed into the system. In some cases without the complete information, the system may not allow the users to go ahead unless some value is entered. This forces the users to enter any value/wrong information in case they are not readily available in the input form. For eg., Account opening form. Hence a complete/detailed input form is a necessity.

b. Completeness and accuracy of updations.

c. Validations of important fields like Date, account numbers etc..

d. Logical Access controls

e. Consistency controls over the data.

3.9 Lack of these controls may lead to data inconsistency problems, unauthorized access etc. This once implemented during the development stage, provides long lasting control mechanism in the application.

4. Unique User-ID

4.1 Apart from the above, each user in the branch should be allotted a User-ID uniquely identifiable with the user person. This User-ID should be tagged to all transactions/activities carried out by the user. Relevant reports may print the User-ID for identification/verification by auditors/supervisors.

4.2 The allocation of User-ID may be made by, the System Administrator along with another senior official under dual authority.

4.3 There should not be any group IDs but individual User-ID should be allotted for proper identification of transactions.

4.4 User-ID should be reflected in all output reports.

4.5 There should be a provision to disable his/her User-ID by the user himself when he/she goes on leave.

5. Addition/deletion/deactivation of Users

5.1 Provision should be available to add new users, to delete existing users (on transfer etc.,) and to deactivate temporarily a user (in case of leave etc.,).

5.2 Appropriate Logs are to be created by the system to know at any point of time, all users' name, deleted/deactivated etc. and the User-ID of the person who introduced the user.

6. Prevention of Access to Operating System

6.1 Except the designated officer carrying out the functions of System administrator no other user can have access to the Operating System and to the Utilities of Operating System. System administrator's access is to be restricted through a Password and strict secrecy is to be maintained. The Passwords of System admin is to be kept in a sealed cover with the Branch In-charge/System Admin under dual custody. This will act as a effective contingency measure in the sudden absence of the System administrator etc.,

7. Passwords/Logical Access to Menus/Data Base by Users

7.1 Access to the network should be restricted at the File server level/Host level and at the Application Software Level as an inbuilt feature of OS/application software.

7.2 Unless the access is allowed by, the LAN Supervisor/System Administrator no user should have access to the System/Package. However Normal Users should not have access to the Operating System since this may result in possible deletion of files/database or direct updation to the database circumventing the application package.

7.3 The access to the package for the Normal User should be allowed only through their Login-ID/Unique User-ID. Each User should allot to himself a Password which should be known only to him/her and to be kept confidentially by him/her. Using the combination of User-ID and his/her Password the User should be given access to "Designated Menu" in the package.

7.4 As a better alternative, access to the Menu could be controlled through work class or user levels instead of through Passwords. Having password based access controls to Menu leads to dilution of password controls.

7.3 There should be facility for the user to change his password frequently by pressing a designated function key. Thus whenever a user feels that his/her password has been compromised or continued for quite some time, he/she will have the freedom to change it without the knowledge and intervention of any body including the System Administrator.

7.4 Apart from the above, the system should force the user to change his password periodically (say every week). This control warning may appear at the time of login by the user. At the end of this period the password will become stale and the user should not be allowed access to the system unless he/she changes his/her password. Apart from the above each user may be given a logical node to access with appropriate time zone. Additionally cashiers may be allotted specific nodes.

7.5 System level logs should record the time at which a user logged into the system and the time of logging out. If a person tries to logon to in any other node not designated to him such unauthorized/unintended access will be let known by this log.

7.6 Further the following additional controls may be taken care of with regard to user-ids and passwords to have better access control:

a. No generic user ids to any user without reflecting actual name

b. Passwords could be alphanumeric

c. No user to exist without any password (System controlled)

d. What cannot be a password (passwords reflecting one's personality etc.,)

e. Not to be written anywhere

f. Password could be changed only by the respective users or the System admin.
Unique password could be accepted - at say 12 rounds.

g. Access may be controlled for non-offices hours/Days reasonably.
h. Storing of passwords in functions keys could be deactivated.

i. Vendor may not be provided with a dedicated profile in system.

i. Terminal level control is possible by restricting number of terminals in the network. Terminal locks prevent a person from getting in to Server through that particular terminal, as the lock has to be opened with a logical key by the user.

8. System Administration Functions

8.1 The functions of System Administrator should be segregated from Normal User's functions.

8.2 Access to System Admin Functions should be through the User-ID of the System Administrator, may be generic or assigned and through a designated password.

8.3 Normal Users should not be allowed access rights as that of System Admin since the Admin functions include maintenance of GL Parameters, Report Names, File Names, Program Names, GL Master Maintenance, Sensitive Program Flags, GL/SUBGL Balance Locking/Release, Mismatch File Maintenance, User Creation/activation/deletion, Node allocation, User-Type Maintenance, Financial Powers to various users and Menu File activation.

8.4 Some of the System Admin Submenus may also be protected with Passwords and dual controls such as requirement of Chief Manager' Password additionally.

8.5 As a better alternative, access to the Menu could be controlled through work class or user levels instead of through Passwords. Having password based access controls to Menu leads to dilution of password controls.

9. Master File Maintenance

9.1 The fixed details relating to various Application areas such as GL, SB, CA-CC-OD, Term Deposits, Loans and Bills etc., are kept in various Master Files.

9.2 The Master File Records are to be protected during creation, modification and deletion. Entry and Authorization are to be protected with respective levels of Passwords of Clerks/Officers/CM etc., Logs are to be created with Pre-Image and Post Image of various fields in the Master File whenever changes are made. Key fields like account No, Account Balance etc., should not, be allowed to be modified for security reasons. File level locking should be implemented to safeguard it from accidental/unauthorized deletion.

10. Parameter Files Maintenance

10.1 "Hard Coding" of various Parameters such as Interest Rates, Service Charges, Commission etc., are to be avoided in the Package as a sensitive security measure to accommodate periodical changes to such rules.

10.2 The Interest Rates on FD, Loans, CA-CC-OD etc., are to be parameterized and changes to the related Parameter files are to be protected by Passwords of appropriate levels of Officers.

10.3 However very sensitive Parameters such as GL Parameters, User Type Parameters, Day-Beg/End File Parameters, Flags such as Inoperative -dormant-closed status flags, Account Range flags etc. are to be additionally protected with System Admin Password.

11. Transaction Processing

11.1 All input transactions are to be protected by controls governed by Double entry book keeping procedures with TOP Down approach with General Ledger on the Top.

11.2 The clerical level users may be allowed only to enter a transaction and not allowed by the package for passing. Passing is to be restricted to Officer level.

11.3 According to financial powers prescribed in the parameters Officers may be allowed to pass a transaction only within the limits allocated to their levels. Beyond this level such amounts/transactions have to be authenticated by a higher level officer or Chief Manager. Thus Security features as in the Manual environment may be enforced by the system in the package.

11.4 Even if simultaneously same account is accessed from different nodes and transactions are input, the Data Integrity is to be maintained by the powerful "Commit and Roll Back" security features. "Dead Lock" situations are to be managed by the package by "Graceful Exits".

11.5 Each transaction is to be tagged with the User-ID of the person who raised the transaction, User-ID of the Officer who passed it, User-ID of the person who corrected it/deleted it and the person who authenticated it along with the time of such raising, correction, authentication and deletion if any.

11.6 As a further security measure, No user who raised a transaction can pass such a transaction if the user is an officer. This ensures dual controls. Cash Receipts and Payments can be handled only by the designated cashier and not by other users. This ensures safety of cash denominations and cash transactions.

11.7 Further precautions

11.7.1 General transactions: Backdated transactions should not be possible or else controls can be built over them.

11.7.2 There can be controls over value-dated transactions.

11.7.3 There should be self-balancing for each transaction - debit should be equal to credit if to be posted or verified. This could apply for batches also. Day-end should not proceed until all transactions are tallied.

11.7.4 Debit transactions should be posted first and then only credit transactions within a tallied batch.

11.7.5 TODs (Temporary Over Drafts) should be verified on the same day.

11.7.6 Preferably, deletion of Posted/Verified transactions should not be possible through the applications, i.e. Every such transaction should be REVERSED through the application. Strict controls should be exercised over the handling of such transactions outside the application i.e. directly on the database through privileged users like ROOT, Oracle etc..

11.8 In system-generated transactions, the system should keep proper control to prevent any unauthorized inclusion of additional entries by opening such transaction.

11.9 At the end of each day, compulsorily the transaction scrolls containing the entire transactions generated at the time of day end is to be physically checked by officers to identify transactions without supporting vouchers, system generated transactions and unauthorized entries.

12. Exceptional Transactions

12.1 All such transactions which are in the nature of exceeding of limits, violations of parameters, concessions given should reflect in a report called Exceptional Transactions Report at the end of the day. This is predominantly applicable to SB, CA/CC/OD, Term Deposits and Remittance transactions. SB-TODs and CA-TODs should also be reflected in the above report. Application software should have inbuilt controls to seek online authorizations from the appropriate levels of officers at the time of allowing such excesses and flag such transaction as 'Exceptional'.

12.2 Interest exception reports should be possible.

12.3 Debits made to restricted accounts like SL (Sundry Liabilities) etc. should be made as exception.

12.4 Exceptions should be generated for such transactions like Operations in inoperative accounts, Huge withdrawal in newly opened accounts, less than minimum balance accounts etc.

13. Interest Calculation/Arresting of Leakage of Income

13.1 For Deposit accounts the Interest is calculated and credited, to all accounts during Half yearly closing/Year Closing according to norms by the system in one go. As and when Interest is due or during closure of accounts also such system-forced calculations are available.

13.2 Wherever the system generated/controlled interest charges/service charges and other charges are computed and loaded periodical test checking of such items may be introduced to have effective manual controls. Whether it is system generated or manually controlled the idea is to prevent income leakage.

13.3 However auditability of such Interest Charged by the system is to be made easy by the "Recalculation " Module/facility inbuilt into the system. The Product Reports are to be very informative to make the review easy.

13.4 Control over the "Interest/Commission Credit accounts" (the account where the contra credit for all the interest debits posted to the Advance accounts is credited through an application as and when the interest is applied) should be adequately ensured. This will have dramatic impact on preventive vigilance.

14. Queries/Reports

14.1 The system generates various reports during the day. These control reports are to be logically arranged through Menus. Some of the reports are generated and preserved in magnetic media and some of the reports are printed, authenticated and preserved as hard copies. Various well documented queries should be available in the package to ensure transparency and checking.

15. Day Begin/Day End/Check Sum Controls

15.1 At the end of the day, Day Book and Trial Balances and other control returns are to be generated by the system.

15.2 The Package should not proceed further if the above are not tallied or if there are pending unbalanced batches, un-passed/partial transactions. This powerful check is in consonance with established accounting practices.

15.3 Without the Day-end process getting over, Day Begin for next day should not take place. Thus all transactions for the day are to be properly accounted for on the same day however large a branch may be. This control effectively eliminates difficulties existed in similar Manual environments.

15.4 The package should generate algorithmically a Checksum at the end of the day. The same is to be checked by the system at Day Begin. These checks and balances will ensure data integrity. The Application Date is to be changed automatically at Begin Day using the Holiday Calendar. No back dated changes should be possible thus.

15.5 Checksum should be part of the data table and not a separate file. The control over the data table should be very strong. Further, if an error occurs in the checksum at the day begin, then the system should not proceed and such situations can be made explicit.

15.6 Once the EOD (End Of Day) is done, the system should be locked for the day, until the SOD (Start Of Day) for the next day is done. SOD for past dates should be prevented.

15.7 The Holiday calendar may not be the same for different parts of the country. The user should be prompted to confirm the date. The software should take care not to allow the future dates. If there is a gap between dates then the user should confirm whether there were intervening holidays and this should be recorded by the system.

16. Consistency Checks of GL - SB - CA/CC/OD Balances

16.1 As a further measure of security the GL Balances/SB Balances/CA-CC-OD Balances are to be locked. No direct up-0dation of balance should be possible.

17. Balancing of Books/House Keeping

17.1 Facility should be provided to generate balances of various GL/SUBGL Heads either on day-today basis or from history files like balances on a given date. There should also be comparative statements giving GL/Sub-GL balances.

17.2 Credit preceding GL Heads (E.g. Term Deposits) should be allowed to go into Debit balance and similarly Debit Preceding GL Heads should not go into Credit (E.g. Loans].

18. Access Logs/Audit Trails

18.1 The Package should provide strong Audit Trails, Access Logs and Transaction Trails to identify which user made what transaction, at what time with special reference to data created, modified, corrected and deleted.

18.2 Master file corrections should be available as PRE-IMAGE/POST-IMAGE reports.

18.3 History Files should be created as an essential feature of the package to create redundancy in data. Reports should be possible from History files as in the case of Daily files. Facility of Purging, Archives should be available after generating backups of selective/sensitive files.

18.4 Audit trail features may be enabled for all the applications.

Eg: sysdba_audit_trail should be true in case of Oracle databases

18.5 There should be an audit trail field for all the DD/TT/Term deposit receipts printed in the application level itself, so that it will be possible to know the details of such activity.

18.6 Audit trail for the activities done by the DBA should be generated on a daily basis.

18.7 Procedures for handling logs and audit trails (periodical purging) should be framed depending upon the sensitivity of the audit trails, requirements of auditors etc.,

18.8 Daily Access logs should be placed to the Branch head for review. It should contain the access made, login failures, access made to the O/S.

18.9 Proper tools for auditing should be provided by way of audit trails, special programs to check direct debits to any GL Head.

19. Anti Virus Protection

19.1 Computer Virus is an impending danger to the data and software.

19.2 The system is to be protected by appropriate "Anti Virus" package, which should be always memory resident. The protection should be available at File Server level and then at the level of Nodes. Regular updates to combat new Viruses should be available to the branches for use along with the Application software.

20. Backups and Contingency Planning

20.1 Most important of all security features is the system of Backups and Contingency planning. Backup of data is to be forced at the end of the day through relevant Menu Options.

20.2 The system of Rotational Backup (weekly cycle) and Permanent Daily Backups/Monthly Back ups are to be enforced for proper contingency planning.

20.3 Well documented Procedures should be available and informed to all branches to have Uniform Back Up practice.

21. User Manual/Circulars

21.1 A detailed User Manual explaining the features and security aspects may made available for every user as soft copy as a menu feature in the Package. Regular updates may be made to the soft copy to enable users to go through them 'on-line'.

21.2 Well-documented circulars may be issued on the subjects of "Uniform Back Up Procedure" and "Printing and Preservation of Printouts" and on various aspects connected with the computerized environment and provided online.

22. Security Features Specific to Application Modules

22.1 Apart from the Security Controls available at Macro Level Global to all Modules there are many Security Controls, which are Module specific.

22.2 SB/CA - CC - OD

22.2.1 Opening and Closing of accounts should have system-generated controls such as requirement of authentication using Officer's level Passwords. The account Number maybe serially generated and allotted by the system. Specimen Signatures may be scanned and related to such accounts, which are used for verification at the time of passing cheques. Products should be generated automatically and during the required periodicity (say, every 6 months for SB and monthly/quarterly for CA-CC-OD) the interest is to be calculated and credited/charged to the respective accounts automatically. TOD Interest may be charged during Begin day for such accounts, which have come to credit the previous day.

22.2.2 System should generate Letter of thanks to the Introducer as well as to the Account Holder on opening of current account. The letters are to be mailed calling for his/her acknowledgement before issuing cheque book.

22.3 Clearing

22.3.1 There should be inbuilt controls for Outward/Inward clearing. Cheque return charges and the value of the returned cheques are to be debited automatically to the respective accounts. Control totals for Inward/Outward clearing are to be generated by the system and tallied with the sum total of individual instruments.

22.3.2 If any mismatch occurs it should prompt before passing.

22.3.3 Inward Cheques details received through Media from Service Branch are to be verified thoroughly before raising debits to the various accounts and to ensure faster generation of possible returns register.

a. Inward clearing: All inward clearing cheques should be debited on the same day
or else day-end should not go through.

b. Outward clearing: Clearing Zones should not be kept open for more than decided
number of days or else day-end should not go through.

23. Remittances (DD/MT/TT)

23.1 Demand Drafts are to be printed automatically by the system after picking the details from the transaction file. The DD Inventory should facilitate correlation of the number available in the system with the actual number on the DD. Missing Numbers if any should be easily detectable.

23.2 The IBR statements are to be automatically generated at the end of the day and a Media/media/network based out put may eliminate the need for data entry at the IBR Cell at the controlling 1 Offices. Accuracy and data integrity may be maintained thus to minimise efforts on Reconciliation.

23.3 Other Precautions

23.3.1 DD printing: Normally reprint should not be possible. Duplicate print should be possible only by higher level user like Branch Manager etc.. Further proper record should be maintained regarding the unused/improperly printed DDs.

23.3.2 The module should incorporate/update data relating to Lost DD Leaves and caution for DDs.

23.3.3 The provision may be thought of in the software to generate check-cipher/test key on the DDs issued so that DD frauds due to alteration of the amount can be avoided. The code may be computed by the system taking into consideration - fields of amount, date, issuing branch code, paying branch code, transactional serial no., etc.. Appropriate manual/system generated access security be ensured to prevent the option from falling into wrong hands/misused.

23.3.4 There should be a proper mechanism to reconcile TTs sent and paid and wherever the TTs are sent through electronic messaging proper encryption of the message to be taken care of by a suitable software.

23.3.5 The software should have provision to cull out entries relating to Inter Branch Accounts, reversals, DDs cancelled, rectifications, direct debits and long outstanding entries to enable thorough scrutiny.

24. Term Deposits (FD/RIP/RD)

24.1 Account Opening/Closing and Interest payments should have rigorous inbuilt controls. FD Rates/Maturity values are to be parameterised and the printing of FD Receipt should be automatic. Periodic Payment of Interest should be automatic and accurate. Transfer to Over due deposits on maturity of the deposit and Checks on Lien marked accounts are certain important security controls.

24.1.1 Term deposit: Normally reprint of Deposit receipt should not be possible, while duplicate print should be available only to higher levels.

24.1.2 The Module should have provision for controlled reprinting of Deposit Receipts in

case of improper printing or partial printing. In such cases, the words 'REPRINTED' may be printed by the system on a specified place on the deposit receipt. Proper records may be maintained with regard to spoiled deposit receipts.

24.1.3 Further, it should close an account (on zero balance) on transfer of balance to another account.

24.1.4 The module should have a provision/built in control to have TDS provision.

24.1.5 There should be a provision to incorporate whether the TDS should be deducted or the whole amount should be paid to the customer on maturity.

24.1.6 All the TDRs opened by the same customer should be available readily added for the TDS purpose. The system should provide for automatic linkage to the other accounts of the same customer so that it will be easier to monitor all the accounts at one time. This will come handy when there is a court order attaching the balances in various accounts of the customer.

25. Cash Module

25.1 There are many preventive security controls to be made available with regard to Cash Receipts, Payments, Denomination maintenance, arriving of cash balance and maintenance of hierarchy such as Chief Cashier/Teller etc.,

25.2 Only after a transaction is raised the denomination can be input by the cashier calling for the specific transaction number given to the instrument/voucher. The denomination controls should be available for exchange of cash across cashiers and those exchanged with customers.

25.3 At Day-end, the Cash balance should be tallied automatically. If any mismatch occurs between actual balance and that generated by the system, Day-end should not proceed.

25.4 The module should be properly linked to other modules such that once the cash account is closed and fully accounted for, there should not be any scope for raising any cash linked entries under single window system.

26. Cheque Book Maintenance

26.1 Issue of Cheque Book may be controlled through the above module.

26.2 Cheque book issue may be entered by the respective clerk and authenticated by the Officer. Cheque Book issue charges are to be debited automatically to the respective accounts. Stop Payments are to be taken care of by this module.

26.3 System should automatically check the serial number with the range of cheque numbers issued to that particular customer

27. Cheques/Bills for Collection

27.1 There should be proper controls on Cheques/Bills for collection so that the proceeds should not be credited/diverted to other than the account originally booked while sending the instruments.

28. Standing Instructions

28.1 Standing instructions for transfer of funds should be automatically done at the period mentioned. All Standing Instructions (including revocation of existing Sis) should be duly authorized for input into the system by use of "Non-Financial Input Forms".

29. Credit Facilities/Loan Modules/MIS

29.1 Proper method of calculation and application of interest on various types of loans and advances depending on the mode of repayment like EMI should be taken care of.

29.2 History of normal interest, penal/overdue interest etc.. should be made available in the package.

29.3 There should be provision for Value dating of credit entries.

29.4 Proper control on Drawing Power/Limit modification under running account such as OD/CC should be provided.

30. Test Databases

30.1 Controls over test databases (Training centres, Implementation offices, Development centres etc.) should be adequate.

E.g. It should not be possible to generate a DD or Advice or Term deposit receipt from these test applications.

31. Data Storage

31.1 The data can be stored in an encrypted form in the database. An encryption methodology can be derived/adopted and the same used for encryption of all data that are sent through floppies or e-mail or any other electronic manner.

32. Periodical Review

32.1 The Application Software features and Security controls are to be periodically reviewed by the concerned group within the bank in consultation with the Computer Audit Cell.

32.2 The feed back received from branches directly or through Computer Audit Reports and through Audit Consultancy Assignments of Audit Firms should be taken up seriously for rectification then and there. Any let up in this regard may lead to computer frauds.

32.3 Suggestions on improvement of security and strengthening of controls are to be taken up with the Vendor/software team and such consolidations are to be released as a New Version. Each such new version may be given a Unique Version Number and loaded to all branches uniformly on a time bound program after initial test run in a few branches.

32.4 The source codes of the programs are never to be parted to the branches and are to be kept in safe custody with the vendor/central office or through suitable Escrow arrangements. Only the Run Time versions should be made available to the branches. Escrow arrangements should be properly documented using relevant Escrow Agreements.

32.5 List of limitations in each application should form part of any document that is given to the users. The users could be made aware of the limitations in this regard in various forums. Procedural controls could be laid down for these limitations.

33. Version Control

33.1 Version control officer should be identified at the CPPD level who will be responsible for releasing the latest version and loading at all the branches concerned. Only latest versions of the software should be running in branches, which will be verified during System Audits.

34. Security Audit

34.1 Security Audit should be done for each module of Application Software in respect of Branch operations including such interfaces connected with ATM Network and Internet banking. This can be done by, the bank as well by a professional organization.

34.2 The preventive controls suggested above may be taken care of through the application software package and the areas are only indicative. Based on application platform and in built security features provided by relevant databases, stringent security controls may be imbedded without losing sight on business flexibility.

Personal Computer (PC)

1. Introduction

1.1 We are witnessing all around proliferation of Personal computers. The PCs have entered the market in India in a big way. We see PCs in shops, business establishments, administrative offices and with many others and at homes.

1.2 It is time for us to gather as much useful hints for uninterrupted and successful computing using computers. The following security aspects will help in proper and efficient use of PCs.

2. Environment

2.1 Heat, Water, Dust, Extreme Magnetism are enemies of computer storage. Please

avoid them. A drop of tea or coffee spilt on your keyboard may damage it permanently. Hence please take precautions to avoid them. The keyboard is to be dusted only by vacuum cleaner and not by using water or any liquid, which may damage the equipment.

3. Dust Free atmosphere

3.1 Always keep a dust free atmosphere near the PCs. Cover them properly after use. Because, even the minute dust particle may damage the Media containing data/information formed out of micro magnetic spots. Also the computer's circuitry may get affected due to dust and moisture and may cause 'short circuit'.

4. Power requirement

4.1 The Computers function with DC voltages. The AC main power is converted inside as DC. Since the computers function with microsecond's speed, the electrical fluctuations will affect the computers. Hence use CVTs (Constant Voltage Transformers)/UPS which work under electronic speed for stabilizing the current to the computer.

5. Power connections

5.1 Invariably the PCs have the following power connections.

1. The PC's system unit is connected to the main power (AC - 250 Volts).
2. The VDU is directly connected to the main power (AC - 250 volts) or the power connection through the system.
3. The printer is connected to the Main power. (AC - 250 volts).
4. The key board is connected to the system unit through a coiled card and round socket.
5. The printer is connected to the system unit through the printer card (wire) through its printer port on the back of the PC.
6. The VDU is connected to the system unit. If any of these connections are missing or loose then the system will not function. Please check up the connections before starting up the computer. Power supply frequency control within tolerable limits is important for proper functioning of Terminals.

6. Power failures

6.1 When you are operating the computers power failures may occur. This will corrupt the files opened and in use at the time of failure. Hence try to save your files intermittently. If possible come out of the package once or twice to take a Media backup. Remember the saying "The value of the Data is felt only when it is Lost'. But we can be wiser to save the Data much before it is lost by proper backups.

7. Switch On/Switch Off

7.1 Unless you come to the operating system prompt or through graceful shutdown, do not power off the computer suddenly. This may corrupt some of the data in use. When you power off a computer, give a little time say 1 minute to power on again. This is to allow settling of the electronic pulses and 'Eddy currents' inside the computer. Also the read write head takes a couple of seconds , after power off, to come to rest. Hence powering ON the system immediately after switching off might jolt the head causing it to rub against the Media surface, resulting in damage to sectors and loss of data.

7.2 When not in use switch off the computer and the VDU. The VDU's have 'tube life time' and the more they are used the less is their life time. Also when not in use the computers will get unnecessarily heated up.

8. Locks

8.1 The system unit has the key board lock. The VDU has an on-off switch. The system unit has a power on switch. These must be set to ON position for booting the system.

9. Booting

9.1 The computer starts up its work through a process called 'Booting'. When you power on the computer please wait for sometime till the operating system prompt C: \ > appears on the screen.

10. Cold Booting and Warm Booting

10.1 Please keep it as a practice to boot the system through the power on key of the system unit. i.e. Cold Booting. Sometimes when the system hangs it is a practice to use combination of keys (such as CTRL+ALT+DEL) to reboot the system. This is called Warm booting. Unless you are thorough, warm booting is to be avoided. In virus affected systems Warm booting is not advised.

11.1 The boot up Media should be kept readily available all the time.

11.2 Appropriate Boot Access Controls (Boot Password) is important for DOS based systems on single user machines (PCs).

11. Lights glow

12.1 When the indicator lights on the Media drive or hard disk start glowing, it is indicative of read write operations of the computer. Do not remove floppies or do any operations with the computer when this is going on.

12. Media care

13.1 Your Media diskette is a flexible one. Hence do not bend them. Always try to preserve them inside the Media jacket provided for the purpose.

13.2 Take care not to fold or twist while inserting the Media in the 'A' drive or 'B' Drive. Some times the Media gets stuck inside the drive. Do not force pull it. Insert the Media cover in the gap between the Media and the drive. The drive spring will get released smoothly. If you force pull it you may damage the read write heads.

13. Media Handling

14.1 Do not touch the Media on the exposed portions of them. These contain the magnetic coated material and the oil in our hand may destroy the coating.

14. Write Protect

15.1 Use always the write protect on floppies containing EXE, COM files and BOOT floppies and floppies containing the DOS utilities. This will avoid accidental erasure of the valuable programs and also it will give protection from Computer Virus.

15. Write Protect - Error in writing

16.1 When you are trying to save a data file onto a write protected Media then a message similar to the above is flashed. Make the Media "write enable" and reinsert in such cases.

16. Removal of floppies

17.1 When you use floppies as default devices for reading and writing, say when you use an Editor (WordStar), after completion of the work, please come out of the package to the operating system prompt by the appropriate command. Without doing the same if you remove your Media and leave the Editor in its default position, the next person using a Media in the same position may lose all his data sometimes.

17. Life of floppies

18.1 Some of the floppies have limited lifetime. The floppies have to be recycled periodically to keep them alive. A frequently recycled Media (i.e. used) will have a lifetime of 3 to 4 years. To do recycling take out old floppies occasionally and try to read them once, at least the directory.

18. Computer Virus

19.1 Computer virus is a dangerous thing that could happen to your computer. Please take care to avoid usage of 'external floppies' and 'guest floppies'. Do not use them without properly checking them for viruses. There are virus detection software called Anti Virus available. There are watchdog programs available to prevent entry of virus into computers. Please use them. The floppies containing EXE, COM files, Boot floppies are to be kept write protected always. The data files have to be stored in separate floppies without write protection. Anti Virus software should be installed in the system. Periodical upgradation of this is necessary as new viruses may enter the system continuously.

19. Daily Backups

20.1 Please be in the habit of taking backups of all your files in floppies and preserve them for future use in case of exigency. A good practice is to have 'Day wise' back ups and rotates them. If by chance somebody erases your files in the hard disk these backups will come in handy. Re-creating the lost files is a monotonous job.

20. Visual Display Unit (VDU/Monitor)

21.1 Constantly seeing the VDU (Visual Display Unit) may tire your eyes due to closeness of bright light spots. Hence it is advisable to use anti glare screens over the VDU to avoid strain on the eyes. Appropriate eye-level positioning of VDUs is important to reduce strain on the Operators.

21. Printer

22.1 Printers get heated up very fast since they are electro-mechanical devices. Hence give them sufficient rest in between sessions. You may use a print sharer to use the same printer between two computer systems without disconnecting the printer connections. Suddenly you may find the printer printing odd characters while printing a regular text. This may be due to loose connections between the system unit and the printer. Set right the connections and use again. There are micro switches available within the printers. These switch settings should not be changed when the printer is 'ON'. Please power 'OFF' the computer and change the settings if needed. Other wise it may damage your printer mother board. The printer should be in "off' position when not in use. Availability of paper and paper feed should be checked to avoid printing on rollers, which may be intentional (if the user wishes to suppress certain outputs).

22. Accidental erasure

23.1 You may some time accidentally erase all your files in your Media by the wild card command say "DEL *.* ". Do not panic. Do not use the Media again. There are special tools available to recover these erased files. The precondition is that before recovering them you should not use the floppies again. It is better to maintain a discipline of using write protect tabs to safeguard against accidental erasure of files.

23.2 These tools should be loaded in to the system.

23. Preventive maintenance

24.1 Like any other machine your PC also needs periodic preventive maintenance. Choose a good agency/vendor who will give maintenance service either on 'Annual Maintenance Contract' basis or on 'call to call' basis. Be with the vendor when he services the machine to get to know the nuances and tips given by him. There is no replacement to 'gained experience'.

24. Best Practices

25.1 Identification of a caretaker for all PCs (where system administrator is not available).

25.2 Declaration by all users that they will take care of all procedures regarding PC security.

25.3 Periodic verification of all PCs by system administrator/care taker for checking,

a. Whether any unauthorized software has been loaded

b. Whether games are loaded (should not have been loaded)

c. Whether unauthorized screen savers/wall papers/image files have been loaded and used.

25.4 If many branches are in the same vicinity, it is advisable to have a resident engineer parked at one of these branches

25.5 Above all, when in doubt it is better to refer to a qualified person rather than to experiment it yourself. Observance of proper computer security in PC operations leads to error free and uninterrupted computing.

Automated Teller Machines (ATM)

1. Introduction

1.1 As technology advancement takes place rapidly in the banking industry, new business channels emerge in the competitive scenario. In recent years Automated Teller Machines are getting installed in large numbers in bank premises and in off-site locations and this paves way for wide choice to the customers to collect the money from the banking system and to avail other satellite services.

1.2 Use of ATM cards and the PIN (Personal Identification Numbers) are effectively supplementing the withdrawal of cash through Cheques and signatures. In turn this has introduced connected risks and the banks have to protect the interest of customers using ATMs and also safe guard the assets side by side. This effectively introduces new preventive vigilance controls for prevention of frauds.

2**.** Safeguards to be taken by ATM Centres/Branches

2.1 Some of the safeguards to be taken care of by the ATM centres and branches are given below.

2.2 **Safe custody of ATM Cards and Pin Mailers and Delivery to Customers**

2.2.1 ATM cards and Pin Mailers are to be sent to branches/ATM centres on different dates by the Card printing section of the bank as per the request from branches.

2.2.2 On receipt of cards and PIN mailers, the branch has to keep them safe in dual control of two different officials. The official having access to Cards should not have access to PIN mailers and vice-versa.

2.2.3 Efforts are to be taken to deliver the cards and pin mailers to the account holders personally without delay against their written acknowledgement/signature. ATM application form to be obtained and retained in the files.

2.2.4 The application form for ATM card to be obtained first and then the card should be issued. If the card and pin mailer could not be delivered in person and if they are sent by post/courier, branches must ensure that first the card is sent by registered post. On getting back the acknowledgement of having received the card by the customer, the signature is to be verified from the application form and then the pin mailer may be sent by separate registered post and acknowledgement received and verified.

2.2.5 This is to ensure that the card and pin mailer are received by the right customer/account holder and they do not fall into wrong hands.

2.2.6 As far as possible, the pin mailer has to be handed over to the customer in person instead of sending through any other mode and the importance of secrecy of pin mailer may be explained to him/her. In the alternative, It is advisable to send ATM Card to the account holder with a request to collect the Password Mailer from the base branch.

2.2.7 At no time, both the card and pin-mailer should be sent together either by registered post or through third party.

2.2.8 ATM cards should be issued only to authorized signatories of accounts having constitution such as partnership, clubs, associations, trusts, companies, etc. as per the policy of individual banks.

2.3 Returned Cards

2.3.1 Returned cards and pin mailers are to be kept under safe custody, till delivered to the customer.

2.3.2 The returned cards/pin mailers are a vulnerable source for commission of frauds and hence utmost preventive vigilance is to be exercised in this regard.

2.3.3 If cards could not be delivered to the account holder due to any reason, these cards are to be cancelled and the relative cards are to be cut and destroyed and the relative Pin mailers are also to be destroyed in the joint presence of two officers.

2.3.4 This is to be marked in the appropriate register and the details to be informed to the card issuing authority as a precaution.

2.4 Hot listing (Hot carding)

2.4.1 The card holders may be advised to intimate, by the fastest mode of communication, the loss of the card to the branch where he is maintaining the account, followed by a confirmatory letter.

2.4.2 Hot-listing/Hot carding facility enables to freeze any operation conducted through lost ATM cards, even if the card is not surrendered to the bank. The particular card, when hot listed, cannot be used for any type of transaction. The ATM should be programmed to capture the card.

2.4.3 In respect of Networked ATMs, the lost card details have to be informed to the ATM network centre which will hot list the card centrally at the Switch level.

2.5 Issue of duplicate cards

2.5.1 A written request should be obtained from the customer explaining the reasons for the request for issue of duplicate card.

2.5.2 The fact that duplicate card is issued in lieu of the original card already issued should be noted in a register or record maintained in the on-line database.

2.5.3 The card holder may be advised to choose a different PIN for the duplicate card.

2.5.4 The card issue program should first cancel the old card and then issue the new
card with a new PIN. This will make the old card invalid.

2.6 Warm Carding

1. If a customer misuses the ATM facility and makes an Over draft by withdrawing tlirough ATM, his card can be made "warm" at the ATM i.e. it will allow only deposits and other query options but not withdrawals till such time he clears the overdraft.

2.7 Withdrawing/stoppage of ATM facility

2.7.1 It may become necessary for a bank to stop ATM transactions in a particular account for many reasons like

a. On a written request from the customer against possible misuse of the card or loss of or damage to the card;

b. At the request of the branch concerned due to irregularities in operations such as drawing without sufficient balance in the account;

c. On receipt of orders from the tax authorities or courts attaching the ATM account;

d. On account of death of the customer;

e. On account of any other specific reason that warrants stopping the ATM facility.

2.7.2 The precautions taken in respect of loss of cards has to be taken in this case also.

2.7.3 The branch should hot list the card in the ATM. This should be noted in the register/on-line data base against the original entry.

2.7.4 In case of networked ATMs, this has to be informed to the network controller for placing the fact in the SWITCH.

2.7.5 An exceptional report for all off-line ATM cash withdrawals should be generated daily and scrutinized for any TOD/misuse of funds.

2.8 **Surrendered Cards**

2.8.1 Surrendered Cards should be punctured in the joint presence of two officials at least and a record may be maintained in a register or on-line data base.

2.9 **Closing of account**

2.9.1 Before closing of any Savings or Current account in a centre where ATM has been installed, the branch should verify whether any ATM card has been issued in the account. If so the card should be surrendered by the customer before closing the account.

2.9.2 If the party desires to close the account with ATM facility and surrenders the ATM card, a notice period of say 15 days should be insisted upon so as to ensure that no claim is pending for any amount drawn using his ATM card.

3. General Precautions and Controls to be observed

3.1 Entry to the ATM room should be restricted and through authorized mechanism only. ATM room should always be locked and under electronic surveillance.

3.2 Prescribed procedures for issuance of Cards are to be meticulously followed.

3.3 Eligibility is to be ensured and lien is to be marked against Deposits wherever such practice is in force.

3.4 TODs arising out of ATM operations to be recovered immediately (and if need be, the secured Fixed Deposits should be closed and liability recovered) The customer can be asked to keep deposit three times the amount of the authorized limit in the ATM. This would take care of the OD for two day.

3.5 Hot Carding should be exercised wherever applicable instantaneously.

3.6 Tallying of ATM cash should be done on daily basis and claims in respect of ATM withdrawals relating to ATM centre branch and non-ATM branches should be done without delay.

3.7 All ATM related GL heads should be adjusted regularly with respective reports and transaction entries outstanding.

3.8 Dual control with regard to stacking of cash, accounting, opening of ATM chest, opening of depository, holding of Keys, safe custody of cards and Pin Mailers should be followed meticulously.

3.9 All prescribed registers should be maintained properly.

3.10 Periodical reports should be sent to controlling offices promptly.

3.11 It should be ensured that ATMs function round the clock and uninterrupted service is made available to users.

3.12 It should be ensured that daily activities are executed by the ATM centres promptly.

3.13 Admin Card and Test Card wherever applicable should be daily used in the ATM to ensure that ATM is functioning properly.

3.14 Insurance cover and AMC are to be kept alive.

3.15 Card distribution to the customers should be done without delay and Cards and PIN Mailers pending for distribution should be maintained securely and under the joint safe custody of respective officials until they are properly delivered to the applicants against acknowledgement.

3.16 Branch officials having ATM cards and PIN mailers should periodically balance and tally the undelivered items under their respective custody. Independent verification by an official who does not have custody of any of these items should also be carried out and recorded.

3.17 Backup of Card base and Files are to be taken on a daily basis and maintained.

3.18 Access lock, UPS, A/C etc. should be maintained properly and trouble free functioning should be ensured.

3.19 Video Surveillance system, Burglary alarms, automatic alerts to local Police Station, should be made mandatory in all the ATM branches. This would curtail the frauds to a great extent.

3.20 ATM related stationery, Consumer Receipts, Journal Printer papers are to be kept sufficiently so as to avoid interruption in customer service.

3.21 User guidelines should be prominently displayed in the ATM cabin for customer reference.

3.22 Dust Bin for customer use should be provided in the ATM cabin, as well as customer lobby.

3.23 Journal Printer Log taken out from ATM daily is to be preserved securely as it provides the basic information regarding all transactions, either successful or unsuccessful. If for whatever reason, the vouchers could not be generated automatically by the back office system, this will come handy in passing the entries manually as this is the proof of transactions carried out at the ATM. These should be preserved as audit trail.

3.24 An analysis of this log will help the ATM centre to guide customers for proper use of ATM facility.

3.25 While the banks should endeavor to provide 24 hours trouble free service for ATM users, it is necessary to put up notice to customers whenever such service is not provided due to reasons beyond control and mention the alternate arrangement. Periodical inspection/audit of this facility is essential.

3.26 There should be a proper Security Keys Management in respect of ATMs, Smart Cards describing the system of holding/custody and operation of security keys. The concept and usage of ATMs in the country are picking up and during the initial stages it is very essential to observe the precautions without exception. All the more it is important to market the concept properly and educate the card holders for increasing the card base and for appropriate usage of the technology. It is equally important to educate the staff members about the Do's and Don'ts of ATM operations which will ultimately pave way for success of the technology and for prevention of frauds in this area.

Preservation of Printouts

1. Introduction

Computerized branches of banks generate considerable number of printouts to satisfy audit/legal requirements. Invariably branches bind the printouts in volumes according to category such as Sectional Day Books, Statement of a/c, Product reports, GL Balance reports, a/c balance reports etc., But there is no uniformity in computerized branches in maintaining the old record register or preservation of the printouts. An organized method of storage and retrieval of these computer generated printouts is very essential for timely availability of information for audit, inspection and supervision. Moreover authenticated printouts form part of legal requirements and an organized set up of storage and retrieval of printouts prevents the banks from embarrassments arising out of lack of evidences.

2. Printing, Preservation and Retrieval

2.1 On the subject of printing, preservation and retrieval of printouts in totally computerized branches, it is observed that there is an urgent need to follow a uniform procedure in view of the following.

a. Large number of printouts are generated/printed in computerized branches and a structured system has to be put in place to store and retrieve these printouts in an organized manner.

b. Uniform procedure needs to be followed by all the computerized branches in this regard.

c. In branches situated in places where the space is a constraint, the storage of the printouts needs to be organized better for optimum utilization of space.

d. The requirements of auditors/inspectors and other officials who require the printouts for their reviews have to be met efficiently without much manual intervention on the part of the branch.

2.2 Some of the shortcomings in unstructured storage of printouts are,

a. Descriptions of the books are written on the face of the bound volumes making it difficult to read, understand and pick up the required record as more and more volumes accrue.

b. Lot of time is spent in locating a particular category of report/for a particular period.

c. Due to unorganised storage the records are, invariably, piled up after a search.

d. Once an old record is taken out for use and is not replaced, it becomes difficult to identify such missing records.

e. Old record register is either not maintained or in most cases not updated properly due to lack of priority to this job and preoccupation with other jobs at the branch.

f. Though the printouts are very important records of the branch, most of the times, no job allocation is made for continued maintenance of the existing/future accruals of records.

g. These printouts are required on a continuous basis by the statutory/concurrent
auditors, inspectors and investigating officers and most of the times the preservation does not facilitate FAST retrieval.

h. In case the branch prefers to remove the old records for elimination after say 8 years, 10 years as per norms, each book has to be gone through individually to ascertain the period/obsoleteness.

3. Preventive Controls

3.1 The following Preventive Control measures will reduce the difficulties of computerized branches to a greater extent.

3.1.1 The printouts accumulated at the end of each month may be collected in one place, i.e. Sectional Daybooks, Scrolls, Product Reports, Day Book, GL Balance reports etc., These outputs should be sent for binding duly authenticated by branch officials under date stamp.

3.1.2 Each category of printouts is to be bound as separate volumes using the services of a professional binder.

3.1.3 Unique running number may be allotted to each volume and written with a bold/black sketch pen legibly.

3.1.4 The bound volumes may be stored in uniform racks or almirahs.

3.1.5 Thus say, in a steel rack with a total height of 7 feet and width of 4 feet we can arrange 6 shelves of 13" each. Assuming the thickness of a bound volume to be 2" we can store roughly 20 volumes per shelf and 120 volumes per rack giving sufficient room for handling.

3.1.6 Assuming 15 volumes are printed out every month by a TBC branch and going by the above logic, one steel rack can hold 8 months storage. Thus 3 racks are sufficient to hold 2 years data and thereafter the records may be transferred to the archives and current/recent volumes can be stored in the same 3 racks. This storing method will save lot of floor space.

3.1.7 Appropriate *'Printouts Register'* may contain an *"Index Page"* and *"Detail Pages".* The Index page will indicate the folio for each category of the printout. Separate folios ("Details Pages") will be opened for each category of printout. A sample of the "Details Page" folio is given in the tables.

3.1.8 Each folio may indicate the "Name of the Printout", "Period of printout" and the "Running Number" allotted to the volume and "Remarks" if any.

3.1.9 The register of printouts may be in the custody of a designated officer.

3.1.10 Review of reports should be done periodically and exceptions handled appropriately.

3.1.11 Appropriate policy for retention of records may be put in place, for the printouts to be preserved as hard copies and in electronic media.

4. Benefits

4.1 Some of the direct benefits of the above suggested methodology are

a. Maintenance of old record register in the format suggested is easy.

b. Numbering the printouts is faster since the system uses the serial number technique instead of printout wise classifications.

c. The description of the book need not be written on the face of the bound volume (only the allotted number be written) thus making the maintenance work easy.

d. Retrieving the printouts and placing it in the rack is only by numbers and hence
very easy and unique.

e. Missing records if any can be located immediately with out much effort by locating
the missing numbers at a glance.

f. Any officer can participate in the maintenance of the old record instantly without
a need for continuity and greater understanding.

g. Space utilization is highly optimized due to standard size of the racks prescribed.
Especially branches having little space will be greatly benefited.

h. After a prescribed period say 8 to 10 years the books need not be kept. In such situations just by seeing the running number we shall be able to identify such books and eliminate them.

i. Locating the books before/beyond a cut-off time say, >3 years, >10 years for removal to the archives is very easy by identifying the number for the cut-off period and all books prior to the number. (The running number is indicative of the period and the period and numbers move along correspondingly).

j. Last of all, identifying entities by number is an established methodology adopted in various organizations such as LIC, Defence, Police and in systems such as SR Number of employees, Examination roll number etc., Also due to the uniqueness of number systems it is easy to register the numbers in memory which enables quick human reaction.

5. Retrieval of Volumes (Printouts)

5.1 In the suggested methodology the retrieval of printouts is made easy through the following steps.

5.1.1 Suppose an officer wants to locate the Outward Clearing Report for June 2001, he has to locate the running number corresponding to "Outward Clearing Report" from the Index page (in this case folio number 17) and then go to the folio no. 17 to locate the running number - in this case - it is 115 . He has to go to the rack and pick up the book under serial number 115 which will be the Outward Clearing Report which he is searching for.

5.1.2 If necessary, in the remarks column in the old record indicate the name of the officer who has taken the book.

5.1.3 Whenever Auditors, Inspectors and other investigating officers visit the branch and seek old records, the old records register will serve as a fast index for identifying the relevant number for the book wanted.

5.1.4 The duftary or sub-staff may be asked to bring the books bearing the required numbers by writing down in a piece of paper by the Inspecting Official/coordinating Officer and this will eliminate any descriptive understanding and will considerably avoid delays.

5.1.5 However since the practice may differ from bank to bank, the best practice is left for the individual banks to decide.

6. Locating Missing Records

6.1 Periodically, an officer to note down missing numbers, locate the same from the work place and rearrange the same may inspect the rack.

6.2 Job allocation can also be made for proper supervision of old records maintenance, since it is easy to understand and implement uniformly across the branches.

6.3 Appropriate guidelines may be evolved for disposal of printouts after certain period and to keep the archives of the same in secured electronic media. This will help in proper utilization of available space.

6.4 The preservation of old records (printouts) in a computerized branch is a very important function. The records serve as primary documents and hence as an utmost preventive vigilance measure the system of preservation should not be overlooked and should be given priority in computerized branches. This will effectively help computerized branches to save considerable time which is otherwise spent in searching the printouts.

Table -**1**

Running Number **Log** * **(Example)**

Calendar month	Running Number allotted to bound volumes	
	Starting Number	Ending Number
April 2001	1	55
May 2001	56	107
June 2001	108	170
July 2001	171	230
August 2001	231	299
September 2001	300	399
October 2001	400	450
Continued	*Continued...*	*Continued....*

The above running number log may be maintained in a folio in the "Register of Printouts". The log will ensure continuity of serial number and will indicate the next number to be allotted to the new bound volume.

Table - 2 Register of Printouts - Index Page

Sl. No	Category	Name of the Printout	**Folio No.**
1.	Daily	Cashier's Payment/Receipt Scroll - Summary	1
2.		Sectional Day Book - Normal (all GL Codes)	**3**
3-		Day Book	**5**
4-		Exceptional Transaction Report	**7**
5-		Transaction LOG - User-ID - wise	**9**
6.		Special Transaction Log - Deleted and Modified Items	11
7-		IBR Summary Report	13
8.		GL Balances Report	15
9-		Outward Clearing Report	17
10.		Possible Returns - **Non MICR or MICR**	19
11.		Drafts Paid/cancelled for a period	21
12.		TTs issued register for a period	23

Sl. No	Category	Name of the Printout	Folio No.
13-		TTs paid for a given period	25
14-		MTs issued Register for a period	27
15-		MTs paid Register for a period	29
16.		BPO issued register for a period	31
17-		OBC - Bills Register	33
18.		IBC Ledger	35
19-		BP – register	37
20.		Bills – customer-wise liability register	39
21.		Cheque BP Ledger	41
22.	Weekly	CA/CC/OD Debit Balances Report	43
23-		Assets and Liabilities Statement	45
24.		Profit and Loss Statement	47
2,5-		Section 42 report	49
26.		Statement of SGL – GL	51
27.		BPOs outstanding as on given date	53
28.	Monthly	CA/CC/OD account balance report	55
29.		SB account balance report	57
30.		Statement of Account - CACCOD	59
31-		Balance of TDR as on any date	61
32.		Balance of ODD as on any date	63
33-		Cheque Book Register	65
34-		Cheque Book Stop Payment Register	67
35-		OBC - Bills Outstanding Bill wise	69
36.		IBC Pending	71
37-		OCC - outstanding – Customer wise	73
38.		BP - outstanding - Collecting Bank wise	75
39-		Bills Overdue - Collecting Bank wise	77
40.		Cheque BP outstanding – Customer wise	79
41-		Overdue – Customer wise	81
42		GL Progressive Report	83

Sl. No	Category	Name of the Printout	Folio No.
43		SGL Progressive Report	8.5
44	**Quarterly**	CACCOD – Interest Rates Printing	87
45		OD/CC Product Reports	89
46	**Half Yearly**	SB - Statement of Account	91
47		SB consolidated interest report	93
48		CACCOD - Folio Charges Report	95
49		SB - Debit Balances Report Any day	97
50		All Users/Active Users/Deleted Users List	99

The above list of Printouts is only indicative. The bound volume may not be sizeable for certain categories like day book. In such cases the branch may combine two or three categories and make it as one volume. Correct classification is to be indicated in the index page.

Table - 3

Details Pages

Sample folios in the "Register of Printouts"

Transaction LOG — User-ID-wise **Folio No: 9**

Sl. No.	Period			Running Number	Remarks
	From		To		
1.	01 - 04 - 2001	To	30 - 04 - 2001	2	
2.	01 - 05 - 2001	To	31 - 05 - 2001	58	
3-	01 - 06 - 2001	To	30 - 06 - 2001	HO	
4-	01 - 07 - 2001	To	31 - 07 - 2001	175	
5-	01 - 08 - 2001	To	31 - 08 - 2001	232	
6.	01 - 09 - 2001	To	30 - 09 - 2001	302	
7-	01 - 10 - 2001	To	31 - 10 - 2001	40.5	
8.	*Continued*			Contd...	

Outward Clearing Report **Folio No: 17**

Sl. No	Period	Running Number	Remarks
1.	April 2001	15	
2.	May 2001	60	
3-	June 2001	115	
4-	July 2001	180	
5-	August 2001	235	
6.	September 2001	309	
7-	October 2001	408	
8.	*Continued...*	*Contd..*	

Statement of Account - CACCOD **Folio No: 59**

Sl. No	**Period**	Running Number	Remarks
1.	April 2001	3D	
2.	May 2001	65	
3-	June 2001	125	
4-	July 2001	190	
5-	August 2001	245	
6.	September 2001	315	
7-	October 2001	410	
8.	*Continued...*	*Contd..*	

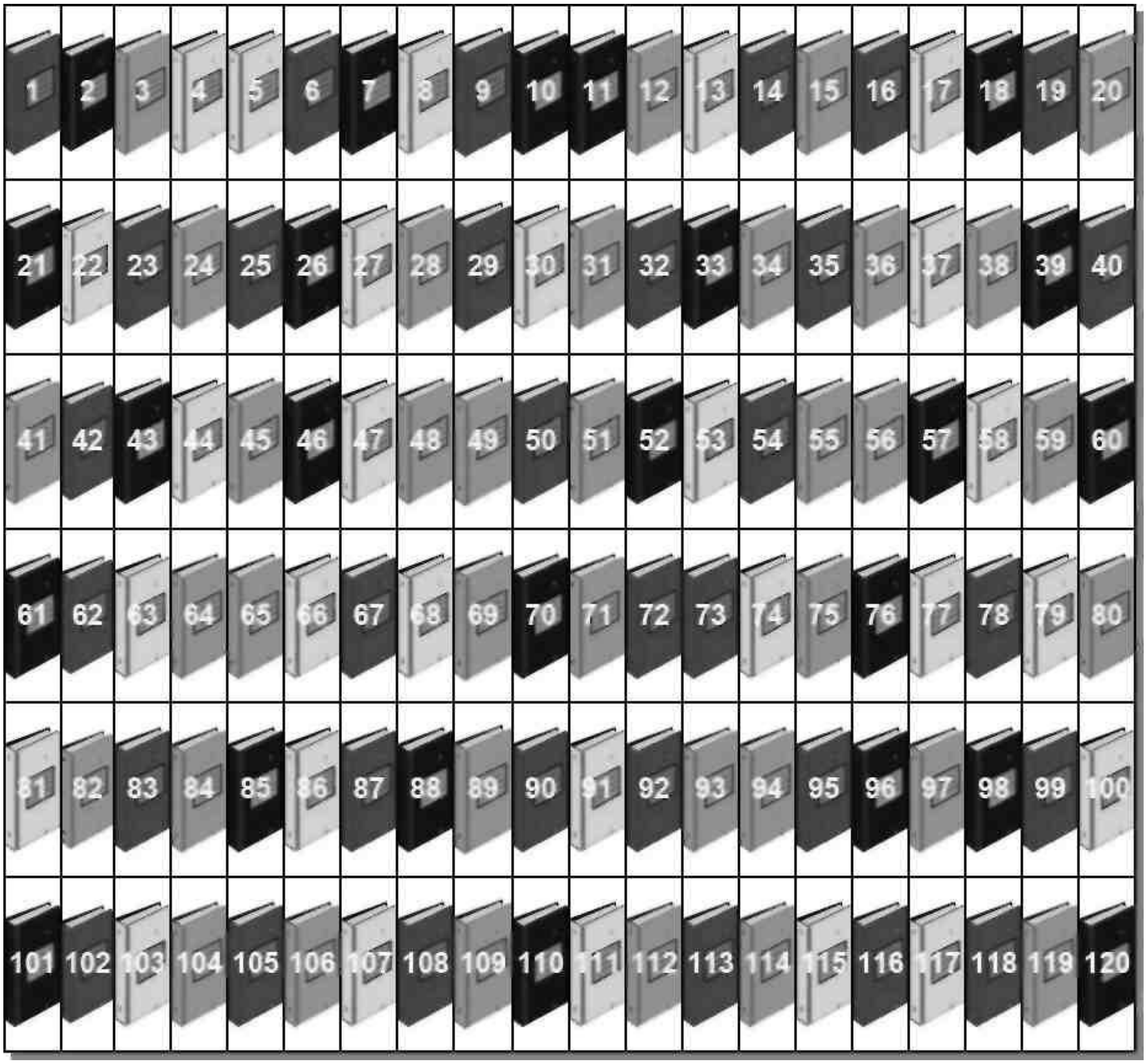
Table - 4 **Method of Stacking of printouts in Steel Racks**

1. Numbers indicate the running number allotted to the bound volumes of printouts.

2. Steel rack of size - Height 7 feet - Breadth 4 feet - Depth 1.5 feet

3. Capacity of the rack - to hold 120 books approximately

4. Assumption - Size of each volume I5"xi2" or 8"xi2" - Thickness of volume 2 inches.



1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120

System Administration - Database Administration

1. Introduction

1.1 Total branch computerization effectively introduces a multi-user environment and there is therefore, a need to oversee constantly certain vital and sensitive parameters by an authorized and knowledgeable person (called System Administrator or Database Administrator).

1.2 Some of the vital aspects of System Administration if taken care of will lead to proper preventive vigilance and efficiency of operations.

2. Maintenance

2.1 Maintain the original software floppies, system floppies, original manuals, Software License agreements etc.,

2.2 Port the latest version of application software and monitor the changes made by the vendors for its authenticity.

2.3 Maintain the inventory of the systems and number the systems to ensure physical safety of the systems.

2.4 Maintain the Computer systems and peripherals/software under proper warranty or under proper annual maintenance contract

2.5 Ensure proper Insurance including Electronic Equipment Policy and Fire Policy.

2.6 Oversee performance channels like e-mail, Internet, VSATs etc.

3. Performance of Computer Systems

3.1 Oversee constantly the performance of Computer Systems and Response time etc.,

3.2 Oversee Hard Disk Space management.

3.3 Supervise Redundancy of Power, UPS systems, Hard disks - Fully Mirrored Status of Hard Disks, Redundancy of Servers - standby servers, to ensure continuity of functions.

3.4 Monitor Disk Performance - Down time, Data Safety

3.5 Periodically Purge old data and transfer the same to archive media.

3.6 Purging of data should be authorized by a password of higher official other than System administrator who will only identify and prepare the data to be purged. Purged data should always be stored in suitable back up media off-line.

4. Password/Access

4.1 Define the rights for users to access specific/group of Menus so that sensitive menus do not fall into every user's hand.

4.2 Overseeing of Password administration.

4.3 Proactive role in maintenance of confidentiality of passwords.

4.4 Maintenance of proper parameters in the system to force periodical change of passwords.

4.5 To meet the exigencies of sudden leave of absence, the Password of System administrator/Super User/Administrator to be kept in a sealed cover and kept under dual custody.

4.6 Restrict the access to Server Console and Server Room to prevent sensitive server functions falling into wrong hands.

4.7 Restriction of usage of External floppies, Games floppies to prevent Computer Virus

4.8 Enabling and Disabling Login during and after office hours to prevent hackers getting into the system remotely.

4.9 Disable provisions of access to Operating System for normal users to prevent them from deleting system files accidentally.

4.9 Maintenance of proper records for all user profile maintenance activities duly signed by the system administrator and authorized by Branch Manager/Officer-in-charge.

4.10 System administrator should not have independent control over sensitive passwords. It should be under the control of BM duly backed up in sealed envelope. It should be jointly used by the Branch Manager/Officer-in-charge and system administrator.

4.11 Records should be maintained in the password usage register for each and every use of sensitive password duly signed by the system administrator and authenticated by Branch Manager/Officer In Charge.

5. Data Management

5.1 Correct Inputs of Branch Parameters/Drawing Power - Interest Rate parameters, Deposit Rate Parameters to be taken care of. Proper updation as per periodical changes to be taken care of.

5.2 Holiday Master files to be maintained properly since banking operations are date sensitive/chronology sensitive.

5.3 Locking up of Master Files for prevention of unauthorized change

E.g. GL/Sub GL, SB/CA-CC-OD Balances Locking

5.4 Complete and accurate maintenance of parameter changes register for all changes

made to system parameters, duly signed by the system administrator and authenticated by Branch Manager/Officer-in-charge.

6. User Management

6.1 Proper inputs regarding User Creation, Activation, Deactivation (In case of leave etc.,) Deletion (On transfer etc.,) and Node Assignment will take care of access identification and transaction identification.

6.2 Unique User-IDs to be distinctly allotted to every user and prescribed financial powers to be attached to such User-IDs or to common levels falling in each group.

7. Backups and Contingency Planning

7.1 Backup Procedures, Periodicity of Backups, Off-site Backups and Data Recovery Procedures are to be taken care of in a planned manner.

7.2 One copy of the latest Data is to be kept in an OFF-SITE location at prescribed periodicity.

8. Vendor Management

8.1 Proper Co-ordination with vendors etc.,

8.2 Co-ordination with other staff members for proper housekeeping and data integrity.

8.3 Liaison with software vendors, EDP departments of banks and Computer Policy and Planning Department for improvement to the application software and for plugging of security lapses noticed in the software.

9. Training

9.1 Training of Second Line for System administrator/Data Base administrator-on-the-job.

9.2 To arrange for training the branch officials in the operations of the package and troubleshooting etc.,

10. Emergency Procedures

10.1 If security violations take place in order to provide an emergency solution, then procedures could be made available to record such exceptions with a time frame for going back to the correct procedure with appropriate ratification.

11. Monitoring

11.1 System administrator should preserve the data and power cable layouts carefully for future maintenance.

11.2 Generation of control reports and reports generated centrally.

11.3 Monitoring of Change of Passwords by users.

11.4 Monitoring of Difference accounts maintained in computers after locking of balances.

11.4 Proper consistency checks provided through Software and Manual controls to ensure data safety and data integrity.

11.5 Monitoring of System controls to arrest Income Leakage.

11.6 Begin Day/End Day Procedures.

11.7 To keep the systems up and available at all times and arranging for repairs and maintenance of the systems.

11.8 To take care of daily routines like day begin, day end, backup, user creation, allocation of nodes etc.

11.9 To do the system related activities for quarter/half year/and year end jobs

11.10 To attend and reply the Computer Audit Report of the branch

11.11 To assist the branch-in-charge in marketing IT related products

11.12 Wherever possible there should be segregation of duties. Different persons should be designated as System Administrator (SA) and Data Base administrator (DBA).

11.13 It is desirable that the SA/DBA are not allotted any financial responsibilities and they are not asked to perform account related jobs and authorization/authentication of transactions.

11.14 As the SA/DBA have access to the Operating system/Data Area, to prevent them from unauthorized access to data base or the software there should be overall supervision of the activities of these officials by other officers not involved in the above jobs.

11.15 The system access logs should be reviewed regularly to detect any unauthorized access.

11.16 Wherever parameter changes are done by the SA/DBA periodic checking of parameters should be done to detect undesired changes.

11.17 The integrated banking environment in branches has introduced many sensitive functions to be managed by system-generated controls. These controls are maintained centrally at one place in the database and are available to many users simultaneously. This introduces a new risk in that any unauthorized change made to this central database will affect system performance at all places. Hence this needs for proper preventive check even at the source data level. System Administration or Data Base administration effectively takes care of this requirement. Hence the Preventive controls enumerated above, though indicative, need to be followed without exception.

Computer Frauds and Computer Crimes

1. Introduction

1.1 Large-scale proliferation of computers and the emerging technologies invading the banking scene have brought new dimensions of risks. Computer Frauds perpetrated by persons of perverse ingenuity, computer crimes carried out using public networks like Internet by trained hackers and other such incidents will shake the confidence and derange the systems and normal working, if it happens, even remotely.

1.2 At the time when banking is in the threshold of cutting edge competition and is looking forward to the state-of-the-art technology to surmount volumes and expectations, more stringent security will choke the flexibility of operations, slow down response time and in turn will affect business decisions.

1.3 There is competition between flexibility and security in view of the incidences of computer frauds and crimes and the computer world is striving to strike an optimum balance.

1.4 Again, prevention of computer frauds is to be carefully planned, in view of more and more lack of transparency of operations of computers and lack of know how and application at various echelons.

1.5 While it takes longer time to formulate set of rules and regulations for a computerized environment, the loopholes get exposed faster than expected due to stray urge for exploiting them.

1.6 However more preventive checks get built into the system based on such experiences and this will take time to settle. It is preferable to proactively address this serious issue of computer frauds and advocate and practice all necessary controls to arrest varying types of risks.

1.7 Here are a few computer fraud related issues, which will throw light on the basic factors leading to commission of frauds and the best way to prevent them.

1.8 By definition, Computer fraud is any behaviour connected with computerization by which some one intends to gain dishonest advantage. It is a deceit by a person by concealing the truth and the injury may be actual or possible.

1.9 The distinct phases of a computer fraud are

a. A wrongful act is committed

b. The wrong doer attempts to conceal or hide the act

c. The wrong doer converts the item to his own personal benefit.

2. Computer related Risks

2.1 The preventive vigilance checks should anticipate and minimize/eliminate the following risks.

2.2 **Software**

a. Unintended lines of code

b. Unauthorized modifications

c. Lack of version controls

d. Unauthorized access to source codes

2.3 **Data**

a. Direct modification to master

b. Lack of audit trails/logs

c. Unauthorized transactions

d. Unauthorized entry/corrections/deletions.

e. Transactions without vouchers

f. Changing data using others' password

g. Willful and wrong inputs

h. Hiding the erroneous outputs

i. Manipulations

j. Lack of checking

k. Unauthorized access to backup media

l. Direct modifications of account balances without routing through transaction processing, e.g. through Operating system commands/special utilities/master balance creation/updation programs left over in the system by the vendors.

2.4 **Access**

a. Stealing others' password

b. Lending the User-ids/Passwords/levels of authorizations

c. Open terminals/Unattended terminals

d. Wire tapping

2.5 **System areas**

a. Crippling the Operating the system

b. Unauthorized changes to the rights and privileges

c. Collapsing System Admin functions.

3. Computer Crimes

3.1 Computer crimes fall into the following categories and mostly relate to e-banking
and networking

a. A person commits a computer crime if he intentionally or knowingly takes, transfers, conceals, alters, damages, destroys, injures the equipment

b. Unauthorized copying of databases or supporting documents

c. Altering services without permission

d. Contamination of computer systems with Computer Virus.

e. Denial of service

f. Disruption of Work.

3.2 Proper access controls, segregation of duties, dual controls, verification of computer generated access logs, checking of audit trails to verify unusual patterns, proper updated usage of anti virus software will all be effective deterrents to prevent or minimize the computer crimes.

3.3 Preventive and Detective control measures should be in place to discourage the potential mischief maker.

3.4 Manual checking of crucial control reports like the exceptional transaction reports and clean over draft reports has to be stressed so as to make the checking a preventive measure for banks.

3.5 There should be proper Job rotation for the staff at periodic intervals so that one person does not remain in a particular seat for a long time. This will reduce the likely occurrence of frauds.

4. Computer related Fraud prone areas

4.1 The following areas of computerization needs concentrated vigil to prevent frauds.

a. System Administration containing sensitive menus and operations

b. Poor Security Policy implementation

c. Control over outsourced products and services

d. Former employees and Current employee activities

e. Vendor products with weak security controls

f. Denial of service attacks through networks - public software

g. Lack of employee awareness and indifferent attitudes

h. Hacking by internal and external sources.

4.2 The computer crimes are carried out by the following categories of persons.

a. *Whizz kids* - making of a genius and perverse ingenuity

b. *Hackers* - one who gains illegal access

c. *Crackers* - one who cracks programs and destroys files

d. *Whispers* - one who listens to telecommunication

d. *Phreakers* - security crackers on communication networks

5. Attitudes - Precautions

5.1 Taking care of the following personalities/attitudes through training program
and proactive guidance will go a long way in arresting of Computer frauds and Computer
crimes.

a. Attitude of *"easy to get away and cannot get caught"*

b. Attitude of *"Stealing a little from big company won't hurt"*

c. Attitude of *"Everybody else is stealing why not me"*

d. Attitude of *"Employer has abused me -1 want to get even"*

e. Attitude of *"beating"* a company/computer system is a challenge

f. Attitude of "If *will not happen to me/us* " syndrome

g. Attitude of computer security not a priority

h. Attitude of *"Three cheers to password'*

i. Attitude of *"Computer will take care of everything - no checking is required'*

j. Lack of transparency of computer operations

k. Lack of Input control - output verification

1. Lack of evidence

m. Lack of Access control - Authorization control - Audit trails

n. Lack of Dual checks in sensitive and high value transactions.

o. Lack of documented Disaster recovery plan/Contingency plan

p. Lack of Business continuity plan

q. Lack of controls - tempted to steal

r. No check on programmers due to lack of transparency

s. Long serving - 'trusted' operators - supervisors - managers

t. Employee vengeance and reasons there of.

u. Bad relationship with the vendor leading to vendor related issues.

v. Missing EDP audit

6. Methods of Crimes and Prevention

6.1 Some of the methods adopted during computer crimes either by using the computer systems or against usage of computers are listed below.

6.2 The activities are self explaining and the activity wise review on routine basis will

minimize the risks arising out of the above.

Sl.	Method of	Activity	Preventive Vigilance
1.	Data Diddling	Changing the input or output unauthorized to conceal or give erroneous	Assigning proper User-IDs -Authentication -
2.	Trojan Horse	Unauthorized but innocent looking instructions imbedded to the programs to	Source code review - Walk thru's -Review of Outputs - Test data analysis.
3-	Salami Technique	Theft of small amounts not drawing attention in a big way.	End value - abnormal value - Null value analysis.
4-	Super Zapping	Data over write or erasing the data base through a program without leaving a	Physical and logical access controls
5-	Trap Doors	Undocumented entry points in the programs switching over to menus or activities not intended to under the prescribed rules.	Program review - Computer audit
6.	Logic Bombs	Destructive programs activating on a	Version controls - Inventory of programs
7-	Asynchronous attacks	Program altered while idle - altering the backup programs and copying the same to live area.	Backups locked up with passwords - strong encryption
8.	Scavenging	Left over information or unattended floppies or unused floppies having sensitive information.	Unused information to be shredded - Unused floppies to be erased before reuse.
9.	Data Leakage	Disclosing the information through	Strong data safety methods - access controls
10.	Piggy Backing and Impersonation	Unattended open logged in terminals getting misused for inputting unauthorized transactions.	Automatic log out of terminals -User discipline.
11.	Wiretapping	Eaves dropping	Fire walls - Network security - Data Encryption standards
12.	Simulation and modeling	Using a backup computer for entering fictitious records	Strong backup procedures - Documented off-site backup procedures

SI.	Method of	Activity	Preventive Vigilance
13-	Computer Virus	"Vital Information Resource Under Siege" - Unusual programs from unknown sources - spread through networks - replicate and destroy and	Anti Virus programs - Watch dog programs Virus vaccines - Anti Virus updates. --- '

7. Hacking

7.1 In the networking arena like Internet, Intranet and WAN, basic hacking involves getting into someplace where one is not permitted to be and seeing things one is not supposed to see. A few common attacks are listed below.

7.2 **Methods of Hacking**

SI. No.	Method	Activity
1.	IP address spoofing	IP packets contain a trusted IP address as their source, but they are not actually from that trusted
2.	SMTP (mail) attacks	Some versions of send mail have bugs, which create security holes. In some mail programs, if the subject line of a message contains the right number of characters (enough to over flow the buffer) the next character is
3-	TCP session	An active session is taken over by an unfriendly user.
4-	Port scanning	All the ports are checked to find any potential security hole with the intent to penetrate your site.
5-	DNS Attacks	Different DNS (Domain Naming Service) attacks can be used to gather network information or overwrite correct information.
6.	Stealing	Stealing network Information and information about others network can be very useful to hackers in planning attacks. Names of computers, accounts, IP addresses and other information should be kept confidential. The security of passwords is particularly important. Passwords can be obtained in several ways.

SI. No.	Method	Activity
7-	Sniffing	Monitoring the network for users to enter passwords as they log on to a remote system. Although the passwords are sometimes encrypted over public networks, it is possible to obtain the original password by running large numbers of candidate passwords through the same encryption function and comparing the outputs to the actual encrypted passwords. This is done either by taking every possible combination of characters in order or by using a large dictionary of common words in the expectation that users will choose common passwords.
8.	Trojan Horse	One type of password stealing technique is referred to as Trojan Horse attack. The user is presented with a log on screen which appears to be genuine. The user enters his user name and password and the log on screen gives an error and asks the user to log on again. In reality, the log on screen recorded the password and closed out, passing the user to actual log on.
9-	Social Engineering	A social engineering attack is the name given to any attack that seeks to trick a user into telling someone a password. For instance, a user might get a piece of mail apparently from the user's service provider or perhaps the company system administrator. The mail asks the user to respond, including the password for the account. It is easy to come up with a convincing sounding reason for this request. Unless the user is aware of the danger, it is easy to be duped. People identifying themselves over the phone as representatives of a service provider cans also trick the users out of passwords. A convincing line from some one "just doing his job" can be hard to resist. Once a password is obtained, hacker will attempt to add privileges to the account and attempt to obtain other passwords and access whatever information interests the hacker. Other network information, like IP addresses and computer names, can be obtained by standard network utilities like ping and fi

SI. No.	Method	Activity
10.	Denial of service	Any attack that is designed to deny access to computing of networking resources is called a denial of service attack. In general a denial of service attack works by overwhelming the system or network with some sort of bogus requests. Some denial of service attacks include the following: **Ping attack** : An unusually large ICMP packet is used in the ping request, exploiting a weakness in the operating system and causing network service to freeze. **SYN Flooding:** TCP connections are established when one system sends a SYN packet to another system, causing the second system to open its end of the connection. SYN flooding uses large numbers of SYN

8. Controls to tackle the above methods of attack

8.1 Knowledge is the first step to any solution especially in a complicated networking environment.

8.2 Strong Fire walls will be able to protect the network from hacking.

8.3 Review of Network security periodically and updating the control mechanisms will help minimize such happenings.

9. Some of the vulnerable areas

9.1 The following are some of the vulnerable areas to be taken care of during inputs to the system:

a. Limit changes

b. Interest rate changes

c. Product changes

d. Accrued Interest changes

e. Payments of Stolen drafts

f. Payment of stopped

g. Duplicate Drafts/FDs issued

h. Opening of New accounts

i. Nominal accounts

j. Inter office accounts

k. Pension accounts

1. Dormant accounts

m. Clearing account

n. Interest provision accounts

9.2 The above areas are only indicative. Most of the frauds can be prevented if only the inputs in respect of the above areas are properly taken care of. It is suggested that in large branches limit changes and interest rate changes could be entrusted to separate officials (Limit Change Supervisor/Interest change Supervisor respectively)

9.3 In case of stolen drafts, if the details are passed on through electronic media, the information/details of the stolen draft will be available to the branches immediately for taking necessary precautions without much lapse of time.

10. Post Fraud Precautions/Evidence Preservations

10.1 In the case of a Computer Fraud, the evidences are many and complicated. Immediately after detection of a fraud, such evidences like data backups, hard copies, history files, current data and other records should be taken possession by the investigating officials without any loss of time and seamlessly. The safe custody of such backups/evidence material is very important. Preservation and testing for its readability and ownership is to be carefully planned and carried out. The acceptability of such evidence as provided for in the recent Information Technology Act 2000 has to be studied and the requirements as per law should be complied with on a continuous basis until the case is closed.

10.2 Any fraud is possible only when there is a matching opportunity. Frauds too have incubation periods. Every fraud is prone to pass through a set pattern leaving behind enough clues. It is the failure to exploit the clues that nurture frauds. A vibrant vigilant culture at the gross roots in the organization will help timely arrest of frauds. We should strive to achieve this to get to near perfection and to put matching deterrents to combat frauds.

Disaster Recovery Management

1. Introduction

l.1 Any computer environment is prone to unforeseen breakdown of key elements such as Power, UPS, Computer systems, Software, data and telecommunication channels.

1.2 It is necessary to provide for a detailed contingency planning and document the procedures, to put the people on guard to meet any exigency.

1.3 A detailed preventive vigilance checklist or a Disaster recovery Management as is popularly called will not only ensure uninterrupted computing but also proper business continuity.

1.4 In fact the disaster recovery plan should be part of the broader Business Continuity Planning. Disaster recovery plan speaks of recovery in respect of computer systems in case of a breakdown whereas Business continuity plan takes care of both the computer environment as well as all other interfaces including manual interfaces.

1.5 The three important factors in a data processing environment are

a. Availability of resources including Data

b. Accuracy, Consistency and Integrity of Data

c. Security of Systems including Hardware, Software and Data

1.6 In a computerized Banking environment more often the integrity of data gets greater focus and security relates to Management's actions to reduce the likelihood of a disaster happening.

1.7 Disaster means anything from loss of a computer file to the total destruction of the data processing facility. As more and more progress is achieved in computerization there is a need to develop a detailed Preventive Vigilance plan to meet any contingency or a disaster.

1.8 The Disaster Recovery Plan should address the following three important issues.

a. Preventive measures to be taken to minimize the likelihood of a disaster.

b. Preparation of an organized response if a disaster does happen.

c. Ensuring business continuity during the interim period of restoration.

2. Areas of Exposures

2.1 The following are broadly the areas of exposures, which need to be tackled.

a. Loss of computer systems and processing capability

b. Loss of communications capability, such as telephone, fax, data, e-mail.,

c. Loss of primary work space/vital facilities

2.2 Although administrative responsibility for functional areas may be controlled by individual departments, contingency planning must be centrally coordinated.

2.3 A well coordinated plan must take care of

a. Interdepartmental interfaces

b. Dependency of one system on others

c. Reduction of duplicate planning

3. Disaster Life Cycle

3.1 The disaster Life Cycle has four-time periods viz.,

a. Normal Operations

b. Emergency Response

c. Interim Processing and

d. Restoration

3.2 **Normal Operations**

3.2.1 **It** indicates the period of time, before a disaster occurs. This section of the plan should include operating practices that tend to prevent a disaster from occurring and those that will help reduce the impact of a disaster, in case it occurs.

3.3 **Emergency Response**

3.3.1 It occurs during the few hours immediately following a disaster.

3.3.2 This section of the plan should indicate activities that may need attention during this time.

3.3.3 It is intended to ensure an organized response and to provide a checklist so that important issues are not inadvertently over looked in the confusion that may accompany a disaster.

3.4 **Interim Processing**

3.4.1 This represents the time during which alternate procedures may be used to support essential business functions until normal processing capability is restored. These alternate procedures which should be developed by functional departments should address, Start-up procedures - Support of essential business functions and Data Recovery.

3.4.2 Start-up section of the Plan should identify specific preparations needed to make the transition from "business as usual" to an interim processing mode.

3.4.3 Support section regarding essential business functions describes how functional departments have agreed to support vital business functions during a disaster recovery period.

3.4.4 Data recovery should cover functional department's responsibilities to retain transactional data (that occurred during the interim processing period) so that files and data bases can be updated when normal processing capability is restored.

3.5 **Restoration**

3.5.1 It indicates the time period given to those activities needed to restore a facility or processing capability to its normal condition. Restoration involves the steps necessary to plan, organise and control these activities.

4. Cost Effective Solution

4.1 The DRP involves discretionary expense. This means that more costly a contingency planning, the more likely that it will be repeatedly deferred.

4.2 Hence it is a cost sensitive issue. Therefore while planning for contingencies focus should be to keep the costs at a minimum and to minimize the testing requirements by encouraging plain and simple business continuity solutions.

5. Priorities

5.1 Business continuity issues should get the priority over disaster recovery plan (DRP).

5.2 Though recovering lost technology is important, we must keep the business running first. Hence business continuity issues take precedence over redundant computer processing capability.

6. Characteristics of a Good DRP

6.1 A good disaster recovery plan should ensure

a. Focus should be on keeping the business running rather than just the computers
running.

b. Plan should contain necessary solutions to deal with problems which need to be tackled immediately and should not worry about problems that are non-existent.

c. Eliminating necessity of costly "Hot Sites" as a cost effective measure.

7. Developing a DRP

7.1 A checklist for developing a good DRP is given below:

a. Objective should be business continuity.

b. Functional Managers be involved in developing the Plan.

c. Front-office staff to be involved while developing the Plan

d. Business recovery first followed by computer recovery.

e. Awareness of DRP and necessary education to precede risk analysis

f. Line Managers to be involved in the maintenance process

g. DRP may be tested periodically and this needs to be effective.

h. DRP is to be reviewed periodically to ascertain the sufficiency.

i. Evaluation of the existing plan by an individual other than the one initially involved in its development.

j. Overall cost effective solution to sustain critical and vital business functions.

8. Implementation of DRP - Backups

8.1 Most important factor in a DRP is the Backup for the various elements of the computerized environment.

8.1.1 *Hardware* - Redundancy of Servers, communication links, nodes..

8.1.2 *Software* — Backup of Current/Correct versions of software - both Systems Software and Application Software.

8.1.3 *Data* - Latest Data Backup with all relevant files and links with integrity.

8.1.4 *Human ware* - Trained Manpower, Alternate System Admin, Alternate Programmers for effective change Management. Alternate to Vendor support.

8.1.5 *Site concerns* - Alternate Site, Power Redundancy etc.,

8.1.1 More sophisticated DRPs could envisage Hot Sites, Hot Standbys etc., Some of the points to be taken care of are

a. Have identical Hardware and network set up so that the software and data can be restored and branch functioning can be started at the earliest possible time.

b. The alternate site should have sufficient hard disk space and memory to enable smooth functioning.

c. There should be a proper publicity for the customers to enable them to transact
business at the new site.

d. For the Disaster recovery plan to be effective there should be periodic drills so that in case of disaster, the plan is put into operation effectively and with speed. This drill is to be done with the branch staff and not with the IT dept personnel.

e. There should be spare stock of peripherals, PCs, Printers and nodes so as to facilitate the use of these items in case of disaster.

9. Backups

9.1 Of the above, the Data Backups are very important. The Banks should strive to document Backup procedures relating to various environments like, Branch Banking, EDPs, Administrative offices, FX installations etc.,

9.2 The Backups should be consistent and periodic. Various types of Backups include On-line backups at *"Hot Sites",* Daily Day end backups on tapes/floppies (Cold Backup), Incremental Backup (Warm backup), Weekly Backup, Month end - Year end backups, Trouble shooting backups, Purge Backups and *"Off-site"* backups. Existence of these types could be taken as a policy initiative.

9.3 One copy of the latest Data is to be kept at an Off-site location at prescribed periodicity. The periodicity of the off-site back up could be daily or at least weekly. It should contain all the data files required for restoring normal business. The day could be say "Friday" or "Saturday".

9.4 Appropriate guidelines be evolved for centralized backup of data in respect of data on stand alone systems in PBA branches.

9.5 The users may be informed about the location of the off-site backups.

9.6 Off-site backups provide great relief during disasters like Fire, theft etc., Hence efforts should be on to keep the Off-site backup (e.g., Backups kept in a nearby office/branch) always current and authentic.

9.7 Test/recycle the backups to ensure they work properly. Clearly defined procedures should be in place to check the integrity of backups.

9.8 Proper framework for preservation of electronic records including media accessibility, time period etc. should be in place.

9.9 Last but not the least is the User awareness of Backup handling and restoration procedures.

10. Data Communication Networks

10.1 Although loss of remote data communication is most likely to happen in conjunction with a disaster that affects computer operations, it could occur alone also.

10.2 Inter branch - Inter office networking of information is gradually being done by many banks in an on-line Real Time Mode (in a distributed processing environment). Hence types of disasters that could occur due to internal and external influences have to be studied in depth in tune with the changing technologies.

10.3 Selection of appropriate media for backup is very important

11. Methodology

11.1 The aim of a business organization is to provide Quality, Reliability and continuity of service to customers.

11.2 Contingency and Recovery planning are keys to continuity of service.

11.3 Although the customer may sympathize in case of a disaster, they will expect provision of normal service immediately.

11.4 Hence a good DRP is to ensure that the customer service remains always undisturbed regardless of any disaster. The customer should have little awareness that a problem has occurred.

12. Steps Involved

12.1 The followings steps are involved in DRP

1. Identification of Risks, primary and single point of failures.
2. *List contact points:* Telephone numbers of all key staff, vendors, customers, controlling offices, police, local authorities etc.,
3. Enlist the supporting services available from EDP, controlling offices, vendors etc. and make all the relevant users be aware of them.
4. Identify the Roles and responsibilities in case of a crisis.
5. *Off-site facilities:* Identify Off-site facilities for operations in case of an emergency.
6. Document the above and provide to key parties.
7. Test the plans/backups to ensure they work.

13. Practical Application of Disaster Recovery Plan In Computerized Branches

13.1 One of the important computer security aspects where greater thrust is given in recent times has been the *Disaster Recovery and Restoration Procedures* and maintenance of *Business Continuity* since the spread of the branches are very wide apart geographically.

13.2 **Data**

13.2.1 The primary concern in computerized branches is the availability of correct data at all times and during on-line-real-time operations the accuracy, safety and integrity of data such as customer details, account details, balance and other parameters are to be maintained, with due care. Appropriate backups will ensure this requirement.

13.3 **Daily/periodical Backups:** Documented back up procedures has to be provided through guidelines/circulars/manuals to ensure the following:

a. Daily backup of entire data residing in the file server/host onto a tape media (DAT backup).
b. At the end of every day, the backup is to be taken in a different tape media and may be rotated on a weekly cycle as a precaution against any bad media error, in case of restoration.
c. Additional backup in the form of compressed ZIP file may be taken in another workstation.

d. Instructions to store the DAT backup in Fire proof cabinets at the end of the day.

e. Instructions to store the DAT backups, in one of the Locker inside the strong room.

f. Apart from the above, permanent backups, monthly backups, backups taken during trouble shooting are also to be preserved for any contingency and check points.

g. Fall back reports containing account balances may be generated and preserved at the end of each day to tackle minor dislocations during start of next day to maintain minimum customer service till the server is made up.

h. Backup should be made mandatory with less human intervention. This can be made a part of EOD procedure so as to ensure all files are backed up.

13.4 **Off-site Backup**

13.4.1 Branches should be instructed to keep one copy of the entire data, say every day/every week, in an off-site location or a different branch, as a precaution against contingent risks like burglary, fire, flood and earthquake etc.,

13.4.2 Where the centre has only one branch of the bank, instructions should be in place to store the Off-site backup in the nearest bank, by hiring a locker.

13.4.3 The controlling offices should monitor the storage of off-site backups, by way of obtention of monthly manager's certificates and through I S audit reports.

13.4.4 It should be ensured that Off-site data should always be up to date, including system programs, application programs, etc. so that recovery can be smooth and complete in case the primary site becomes inaccessible or completely destroyed.

13.4.5 The users must be told about the location of the off-site backups.

13.4.6 The aim of the above backup and restoration procedures, has been to create sufficient redundancy in respect of data with proper date and time stamps, to enable computerized branches restore the data in time and restart the operations, within the quickest time possible, from the moment disaster occurs.

13.6 **Software**

13.6.1 In addition to the data, branches should be advised to take regular backups of software executable files in tape media and preserve. In case of need for recoveiy, they will be able to restore the software from these tape backups. The copy of the same set of execu-tables should be available in nearby branches and at the Head office to maintain sufficient redundancy in respect of software.

13.6.2 In the case of in-house maintenance, source code of the software is to be maintained centrally and one copy of the same should be kept as Off-site backup. The backups of the source code may get updated/replaced with latest updates periodically, say once in a fortnight. Proper access/authorization controls should be exercised to ensure that the source code does not fall into wrong hands.

13.7 Hardware Failures

13.7.1 The critical element in the TBC branches is the File server or central host. The file server provided to TBC Branches should have inbuilt features for Hard disk mirroring. The twin hard disks may be mirrored in real time during the operations. In case of failure of one hard disk the other takes on automatically and will provide the necessary redundancy.

13.8 Standby Servers

13.8.1 The branches may be provided with a mirrored server as hot standby. In case it is not provided, the following solution will take care of any failure of the main file server.

13.8.2 To take care of contingencies like total failure of the main server in TBC branches, arrangements may be made to have a Stand by server and at the end of the day, the data from the main server may be copied to the standby server, to keep it in ready condition.

13.8.3 Controlling offices may also be equipped to have one or two such Stand by Servers at their offices to cater to such exigencies of branches, as a fallback.

13.9 UPS

13.9.1 The other critical element is the power supply and uninterrupted power to the computer systems for the continued running of the branches.

TBC Branches may be provided with Two UPS systems of similar capacity. In case of failure of main power supply, the UPS will take on automatically using the battery backup. In case of failure of One UPS system the second UPS will provide the necessary backup to continue the operations.

13.10 Fire, Theft and Burglary

13.10.1 Extensive instructions may be given to the branches in consultation with the Security Department with regard to Fire safety measures and to protect the branches against burglary.

13.10.2 The branches may be provided with fireproof cabinets for safe storage of tape backups and to protect the backup data from Fire hazards.

13.11 Computer Virus Protection

13.11.1 The file servers and nodes of TBC Branches may be protected through appropriate provision of Anti Virus software, both server version and node versions. Regular updates are to be provided through vendors. Through Intranet, regular anti virus updates may be provided wherever possible.

13.12 Insurance and AMC

13.12.1 The computer systems should be insured through Electronic Equipment Policy and Fire Policy for the replacement value and comprehensively major risks are to be covered to protect the systems. Annual Maintenance Contract may be ensured for all the systems to extract timely support in respect of breakdown calls.

13.13 **Handbook on Disaster Recovery Procedures**

13.13.1 As a further proactive measure and to educate the personnel on the consequences of disaster in a computer environment all the computerized branches may be provided with the 'Do's and Don'ts' to meet any emergency situation and during various types of disasters. This will keep the personnel always in full preparedness to meet any situation.

13.14 **Restoration Procedures**

13.14.1 The threat to a computerized branch could be either total loss of site like in case of earthquake etc., or disaster to any one of the elements of computerization like failure of power, lightning strike, sudden failure of file server or loss of data due to file corruption, virus etc.,

13.14.2 Sufficient redundancies should be built in to protect and restore the data and other resources in case of above failures within the quickest possible time to maintain business continuity.

13.14.3 The personnel should be educated as to how to restore the data and other resources from the backups available.

13.15 **Disaster Recovery Drill**

13.15.1 To keep the branches in readiness to meet any exigency with confidence, they may be instructed to conduct a *'Mock Disaster Recovery Drill* periodically and record the observations in branch records. The copy of the record may be made available for IS audit etc.,

13.16 **Other Best Practices**

13.16.1 However, in view of the concerns expressed towards computer security globally, in recent times, the following additional steps may be undertaken.

a. A set of full hardware/software backup facility may be provided at a central location by replicating the branch system where there are more number of branches in a cluster. This will effectively introduce the "HOT SITE" concept in case of any disaster recovery.

b. A Task Force for Disaster Recovery Management may be formed to discuss in detail the subject and prepare such manuals for guidance of branches. Relevant Excerpts from the Disaster Recovery Manual should be shared with all users, so that in the event of a disaster striking, all the users know how the system and data should be recovered. Also, the residence telephone/cell phone numbers of Disaster Recovery Team members and Vendors should be made widely known to all users, so that they may be contacted in emergency situations.

b. It may be reiterated to all controlling officers to keep sufficient number of standby servers/peripherals in readiness to effectively handle any situation arising out of dislocations in TBC branches.

c. With the existing and proposed network, the data backups through secured methods may be taken and preserved in designated off-site file servers for online restoration in case of need/emergency.

d. The access to backup floppies/magnetic tapes should be made available to branches including holidays.

e. CD-Writers may be provided to designated branches to be effectively used for preparing compact backups including history files for easy storage and restoration.

f. Mock recoveries and dry runs may be insisted from random branches in each area prone to disasters to keep them in readiness to face any situation of disaster and for structured and speedy restoration and business continuity with minimum possible dislocation.

g. Systems audit should be carried out at the computerised branches and other data centres from time to time covering critical computers and communication systems so that any loopholes in the disaster recovery system can be fixed.

h. A mechanism should be developed for reporting all the incidences of system interruptions to the next higher authority so that immediate remedial action can be initiated.

13.17 The reasons for disasters are many, but invariably they are found to be man-made or man-caused and therefore preventable. At first sight they may well appear to be unavoidable but with proper awareness and preventive measures these can be avoided. With the Information Technology expanding every day the disaster is always 'lurking round the corner' and there is no place for complacence. Hence people working in IT environment have to work with anticipation and preventive vigilance for better management of potential disasters.