Information Security Policy

Need Assessment of Information Security Policy

Technology adoption by Jhalawar Kendriya Sahkari Bank Ltd. Jhalrapatan has led to the delivery of the modern banking services to the valuable customers of the bank. Technological innovation is the key tool to drive financial services to the unreached population. In order to maintain secure financial transactions and ensure transparency, safety and security in baking and financial transactions, there is a need of the Information Security Policy (IS Policy). There is also an imperative need of the Information System Audit (IS Audit) at periodic interval for mitigation of risks emanating from adoption of new technology.

With usage of the core banking system to offer banking services electronically there is a need to place the internal control systems for ensuring safety and security of the information system. The Information System Audit (IS Audit) shall form part of the Internal Audit/ Inspection. In order to operationalize proper IS Audit mechanism, broad guidelines have been formulated in this policy.

With banking operations migrated to IT environment, it is pertinent to put in place appropriate and robust IT policy and IS Policy with adequate emphasis on IS Audit.

Physical and Environmental Security

Policy

IT resources of Jhalawar Kendriya Sahkari Bank should have proper physical access controls to protect information assets and data processing activities from unauthorized access and environmental threats

Procedures

P.1 Exclusive operation areas shall be away from the flight paths, power lines, potential terrorist targets, powerful transmission centers, etc.

P.2 Information processing facility along with all the assets it contains shall be insured suitably for adequate risk transfer.

P.3 The placement of various computers and furniture should be so arranged that free & quick movement of people is easily possible when required to evacuate the premises.

P.4 Only authorized personnel shall have access to Information processing area.

P.5 Record of entry and exist must be kept and retained for exclusive operations areas.

P.6 Movement of all computer systems, components, parts and media from Jhalawar Kendriya Sahkari Bank’s sites shall take place only with the permission of competent authority.

P.7 Information processing facilities must have adequate measures to fight the incidents of fire.

P.8 Exclusive operation areas should also have smoke and heat detectors.

P.9 Fire instructions should be clearly posted. Fire alarm buttons should be visible and accessible in case of such incidents.

P.10 Training on usage of firefighting equipment shall be provided to the users and the fire drill should be performed at infrequent intervals.

P.11 Evacuation plan should be documented and rehearsed at infrequent intervals.

P.12 Room temperature and humidity levels, as specified by the manufacturers shall be maintained in the exclusive operation areas. The same shall be managed to the possible extent at other operation areas.

P.13 Provision for clean and adequate, uninterrupted power supply for computer systems shall be made.

P.14 Access violations must be recorded and escalated to higher authorities for appropriate actions. The procedures to be followed in case of access violations should be as per the procedures given in the section on Incident Management.

P.15 Terminals should not be left un-attended in a logged in status. However, servers on which various processes may be running during operations need not have continuous manual presence but shall be kept under lock and key. Super user access to these servers shall be permitted through console only.

P.16 Information processing facility area should have smoking restrictions. Appropriate sign should be displayed at conspicuous places.

P.17 At exclusive operation areas provision for another source of power supply like diesel generator set shall be provided.

P.18 Alternative air-conditioning arrangements should be available at exclusive operation areas.

P.19 Hazardous commodities should not be stored within Information processing facility area.

P.20 Installation of appropriate access control like password, swipe card/ bio-metric devices, etc. should be considered in the light of the criticality of the information assets. Access to visitors to exclusive operation area shall be through electronic access cards and recording in manual register at the entrance. This access shall be subject to permission of IT Head. Access to server room, networking area shall be for authorized persons only. Installation of video surveillance with recording equipments to monitor the entrance and movement of personnel inside exclusive operations area is recommended. Mobile phones (Except those provided by the Jhalawar Kendriya Sahkari Bank to its employees) should not be allowed to be carried in the exclusive operational area, particularly where the servers & networking equipments are kept.

User Accounts & Password Security

Policy

The User Id's (identification) must be so managed as to reflect the respective employee's role-based privileges and to ensure the accountability for tasks performed.

Procedures

P-3.1 Privilege to register a new user account will be confined to the respective head of the concerned branch / office of the Jhalawar Kendriya Sahkari Bank Ltd. Jhalrapatan

P-3.2 User profile register should be maintained and updated while creating a new user ID.

P-3.3 Acknowledgement shall be taken from users at the time of allotment of user ID.

P-3.4 Each user will be responsible for all activities performed with his / her user ID.

P-3.5 With the exception of reserved user accounts created for the internal use of the operating system, RDBMS, application system etc., all other accounts should be uniquely identifiable by the respective user's name.

P-3.6 All users should have unique user ID and no user should have more than one user ID. However, in case of exigencies at branches having limited staff, an officer may be allowed two separate sets of privileges temporarily. Rules related to such cases like permission and follow up procedure shall be clearly defined.

P-3.7 Privileges of each person across various layers of software (like OS, DBMS and application software) shall be within the authority placed in that person by the Jhalawar Kendriya Sahkari Bank Ltd. Jhalrapatan

P-3.8 User ID of a person on leave/under suspension/deputation to other office should be got deactivated during his period of leave / absence/suspension/deputation.

P-3.9 User ID must be permanently disabled, when the concerned person has retired or dismissed from the service of the Jhalawar Kendriya Sahkari Bank Ltd. Jhalrapatan

P-3.10 Default user accounts like ‘Guest’ will be deleted. This shall not be applicable to user accounts like SYS, system used for administration of database as a default user.

P-3.11 Default passwords provided by vendor / generated by system at the time of user registration should be changed immediately on first time login.

P-3.12 Passwords must not be left blank.

P-3.13 No recycling of passwords will be allowed for a minimum of four cycles.

P-3.14 In case if the user has access to multiple applications, systems, resources, etc. different password for each of them should be used.

3.3. Implementation Guidelines

Users should follow the guidelines related to Password formation given below**:**

Password should be of minimum 8 characters in length.

Password should contain both upper and lower case characters (e.g., a-z, A-Z)

as well as digits (e.g., 0-9), i.e. it should be alphanumeric.

Same character should not be repeated in continuation in the password.

The password should not be a word found in any dictionary (Vernacular, English

or foreign)

The password should not be a common usage word such as computer terms and words indicating Jhalawar Kendriya Sahkari Bank Ltd. Jhalrapatan name, “password”, etc.

The password should not indicate personal information (like User ID, birthdays,

telephone or vehicle numbers, names of near and dear, etc.).

4. Segregation of Duties

Policy

A distinct resource for each activity needs to ensure the principle of segregation of duties.

Procedures

There are many instances where two parts of an activity or an asset have one control each that contribute to security and hence it is essential to keep these two or more parts separate, failing which the compensating controls get diluted and tend to be compromised. Segregation of tasks / duties should be done in the following cases:

1 The posting of transaction and authorization of the same shall be done by different persons, i.e. maker and checker should not be the same.

2 Person(s) undertaking the review of audit logs should not be the same whose activities are being monitored.

3 Operational responsibility for networks should be separate from computer operations.

4 Production and issuing function for cards must be separate from production and issuing function for PINs

5 Security administration and Network administration functions should be segregated.

Network Security

Policy

Network of computing resources will be deployed in a secure and need-based manner with requisite manual, automated and procedural controls to provide a reasonable assurance that benefits of connectivity are not counteracted with compromise of confidentiality, integrity and availability of data or any other resources.

IT Department will depute a Network Administrator for managing data centre's network will be single person or group of people.

Network Topology

P-5.1 Network architecture will be planned and documented.

P-5.2 Mission critical connectivity and hardware for the same will be redundant to provide continuous connectivity. The decision about an activity falling into mission critical category will be decided on business requirement and with the approval of management or its delegated representative.

P-5.3 Any change in the architecture of the original network, other than new addition shall be made after approval as mentioned in point (P-5.1) above.

P-5.4 Standby hardware for replacement in the network area shall be arranged for either by stocking the same or in the form of SLA agreement with an outsourcing agency.

P-5.5 Only authorized staff of Jhalawar Kendriya Sahkari Bank and Vendors will be allowed to change network architecture.

P-5.6 Only authorized staff of Jhalawar Kendriya Sahkari Bank and Auditors will be allowed to review the network architecture.

P-5.7 SLA and confidentiality agreement will be signed with all the authorized personnel and agencies prior to giving them access or information related to data centre network.

P-5.8 Any planned change in the network should be discussed on need basis with vendors of servers, routers, firewall, maintenance agencies and connectivity providers, prior to implementation. (This will help in identifying problems if any due to change, load on bandwidth, uniform implementation and restriction from any external agencies.)

Network Access

P-5.9 Multiple logical networks may exist on one physical network.

P-5.10 Production network will be logically separated from test network and any other network that may exist (separate IP schemes to be defined for Production and test network and for any other network if available).

P-5.11 Access control rights will be defined to control users from one network to access resources on another network.

P-5.12 Access control rights will be planned and documented. It should be approved by Management or the delegated representative of the Management.

P-5.13 Change in access control will be approved by Management or the delegated representative of the Management prior to any change.

P-5.14 Only authorized officials / vendors will have access to ACL (Access control list).

P-5.15 AAA servers may be used to authenticate users.
P-5.16 Resources that exist on the network (viz. Hard disk, CD-ROM, Printers, etc.) will be shared on need-to-use basis and shall be available only to authorized users.

IP Numbering

P-5.17 IP Numbering methodology will be planned and documented. Management or the delegated representative of the Management should approve the same.

P-5.18 All IT resources, which require IP on the network of Jhalawar Kendriya Sahkari Bank (including LAN and WAN) will be provided IP numbers from the identified applicable range.

P-5.19 All IPs from the available pool of IPs at Data centre building, that are not issued to any resource will be disabled at router / gateway level. When any IP is issued from the reserved pool, activation of the same will be done.

P-5.20 Polling (i.e. trying to ping IP to get its response) to critical locations IPs will be done periodically. Results of the same will be helpful to identify status of resources connected to the network.

P-5.21 IT resources that connect to outside network may use technology to hide its static IP (i.e. masking original IP to prevent outsider from knowing the IP in use).

P-5.22 IP of the any IT resource will be changed after approval of Network Administrator.

P-5.23 Any change in IP addressing will be done in consultation (wherever required) with concerned agencies. If the change is made for temporary time period, it will be restored to original state in stipulated time.

P-5.24 All services available on equipments will be listed with consultation with vendor and/or manual provided.

P-5.25 Services identified and approved will be activated on auto-start / manual start basis. All services other than approved, on each resource will be de-activated.

P-5.26 Review of services running will be made periodically. This review may be done manually or using automated tools.

P-5.27 Any change in status of services will be approved by network administrator prior to change. Necessary controls will be applied to restrict enabled services. Actions taken to enable / disable the service and applied controls will be documented.

P-5.28 Services like FTP, Telnet, Terminal Services or any other remote login should be enabled based on requirement and should be available to authorised users only.

P-5.29 Static IPs should be configured on all resources. Services like DHCP that allocates Dynamic IPs should be disabled.

P-5.30 For internal use Private IP address ranges should be considered.

Switch & Router Configuration

P-5.31 Configuration of Access Control List (ACL) for Switches / Routers will be planned, documented and approved prior to installation.

P-5.32 Security audit logs, incident reports, and on-line reports will be reviewed on pre defined frequency.

P-5.33 A separate sys log server to be configured.

P-5.34 Router tables will be maintained securely in the router.

P-5.35 Login IDs and Passwords for router and switches will be treated as sensitive information and will be managed by authorised administrators.

P-5.36 All changes to router table entries will have an independent review on periodical basis.

P-5.37 Access violation, if any, will be documented and escalated to higher authority and acted upon in a timely manner.

WAN Security

P-5.38 Different offices, PCs, Offsite-ATMs, etc. will be connected through WAN using leased lines, ISDN, VSAT or any other media that connects point to point with branch-to-DC or branch-to-POP of subscribed VPN only. Use of public infrastructure viz. Internet if used for connectivity should be used only with prior approval of Management or its delegated authority, but also after ensuring the security of data as well as network.

P-5.39 Data transmitting from one point to another should be encrypted using industry standard algorithm authorized under prevailing IT Act.

P-5.40 Fallback from one media to another in case of failure will be provided for connectivity for critical locations.

P-5.41 Connectivity may be taken from multiple service providers.

Branch LANs

In addition to above procedures, the following procedures need to be followed which are connected to Data Centre (DC) without Servers and with servers not connected to DC.

Connected to Data Centre

P-5.42 Branches that provide inter connectivity between PCs installed in the branch will ensure sharing of Hard disk, CD-ROM, CD-Writer or any storage media is not enabled unless authorized by the PC owner. (Branch PCs will have some amount of local storage viz. daily balances in softcopy, scanned signatures and photographs. This should not be shared unless authorized.)

P-5.43 When sharing is enabled controls will be placed to allow access to only authorized PCs to the designated resource.

P-5.44 PCs at the branch will have access to only specified servers and services.

No Connectivity to Data Centre

P-5.45 Branch Server’s resources will be shared on need-to-know and need-to-use basis. User wise access rights will be defined for accessing data from the server.

P-5.46 Resources among user PCs will be shared on need-to-know and need-to-use basis.

Miscellaneous

P-5.47 Minimum configuration for any device/link on Jhalawar Kendriya Sahkari Bank’s network, including levels of encryption will be defined. Review of the minimum configuration will be made on periodical basis to identify any change required.

P-5.48 Devices / links will be procured on the basis of defined minimum configuration. Deviation, if any, will be identified, documented and compensatory controls will be set to overcome risk if any.

P-5.49 Backup of router and switch configuration will be maintained at the network centre.

P-5.50 Any unused wall mounted sockets should be sealed off and their status should be formally noted.

Anti-Virus Controls

Policy

Antivirus policy should be an internal IT policy which defines anti-virus policy on every computer including how often a virus scan is done, how often updates are done, what programs will be used to detect, prevent, and remove malware programs. It defines what types of files attachments are blocked at the mail server and what anti-virus program will be run on the mail server. It may specify whether an anti-spam firewall will be used to provide additional protection to the mail server. It may also specify how files can enter the trusted network and how these files will be checked for hostile or unwanted content. For example it may specify that files sent to the enterprise from outside the trusted network be scanned for viruses by a specific program.

Procedures

1 The anti-virus product should be operated in real time on all servers and client computers. The product should be configured for real time protection.

2 The anti-virus library definitions should be updated at least once per day.

3 Anti-virus scans should be done a minimum of once per week on all user controlled workstations and servers.

4 When A client/Server detected any harmful virus it client should be removed urgently from the network.

5 No outside floppy/CD ROM should be allowed in the computer without scanning.

Implementation Guidelines

There should be an anti virus server with latest update.

Digital Signatures

Policy

Digital Signatures affixed by both human and computers will ensure authentication of the source, confidentiality of transmitted message and integrity of message to fulfil the contemporary requirements of technical and legal nature.

Email Security

Policy

All E-mails will be handled in a secure manner and the security level must be commensurate with the data and / or message transmitted. The email server should have additional protection against malware since email with malware must be prevented from entering the network.

E-Mail Address Policy

The major problem that is to be resolved in giving the e-mail addresses to the users is to ensure the address resolution when multiple similar names occur, which is a common occurrence. This problem is found to occur in every nation and therefore there are some proven name resolution methods that have been used by many of the service providers.
There are two major naming methods that are used in India. In some parts of India, the “surname” or the “family name” is used to address a person. In some other parts (though in a few states) the “given name” is used for addressing a person. In one state, one gets to see the usage of a large number of initials attached to a given name. Therefore, unlike in the west, where the naming mechanism is uniform, we need to take the differences in the naming mechanism to be reflected in the e-mail addresses so that the address resolution problem is properly taken care of on an All India Basis.

E-Mail Usage Policy

The electronic mail system is one of the most useful discoveries/ inventions of the Cyber age and is associated with pitfalls of like magnitude. In this rapidly changing cyber space technology scenario, Mail System Administrators try their level best to keep the systems secure enough so that it is not misused by the hackers. In spite of their (administrators’) best effort new virus/worm and spam mails get into the mailboxes of the innocent mail users. The recipient of the e-mail should verify the authenticity/ genuineness of the e- mail after receiving use the e-mail and delete unwanted e-mails from the mailbox. Keeping the virus (so called time-bomb) problems in view the mail store should not be considered as the safe repository for the sensitive/ useful data. Lastly the messaging system (analogous to the dispatch section) should not be confused with the electronic record management system (analogous to the record room) comprising of non-editable / read-only digital files.

Backup and Restoration Control

Users are responsible for taking backups for their individual's Desktops/Laptops.

Information owner in conjunction with System Administrator/ NOC Team should identify the critical Server resources that need to be backed up.

Appropriate backup media should be chosen by Information owner based on the criticality of data and retention period.

Periodicity of backup (backup schedule) should be determined by Information owner and the backups of Critical server resources should be taken by System Administrator/ NOC Team as per the schedule.

Backup logs should be regularly maintained and kept up-to-date and it can be in the form of hard or soft copies

All backed-up resources should be stored in safe (fire-proof cabinets) and protected place.

Critical server resources backup should be maintained in off-site location, away from the Primary site.

Backup/Retrieval logs should be reviewed by the respective system administrator to ensure proper backup.

Sealed envelopes with signature should be used for transporting media to identified off-site location.

Third Party Access Controls

Policy

Access to Jhalawar Kendriya Sahkari Bank's computing resources by the personnel / computers of any organization other than Jhalawar Kendriya Sahkari Bank , will be granted on business merits and executed in a secure manner.

Procedures

1 Decision of Third Party access will be allotted strictly on the need-to-use basis to support the business case.

2 The access privileges (like what data to be accessed, through which software functions that data is to be accessed and what access rights are to be granted) will be decided by Jhalawar Kendriya Sahkari Bank on the merits of the case.

3 A suitable agreement / undertaking should be executed with the concerned parties before granting access.

4 Wherever necessary, the confidentiality clause may be included in the agreement.

5 Proper record of third party access should be maintained and reviewed on periodic basis.

6 Right to inspect third party's operation area may be a part of the agreement / undertaking.

Data Centre Security

Policy

The Data Centre must have utmost security measures to justify the crucial business and technological assets it houses and to protect from the risks inherent to the massive single point concentration of Jhalawar Kendriya Sahkari Bank's transactions. These security controls will be reviewed and refined on an ongoing basis to provide an assurance of continuity of operations.

Procedures

P-11.1 In the central State Co Op Banking solution scenario, the Data Centre happens to be a focal point, with a high concentration of the State Co Op Bank's IT resources like data, computing power, networking, etc. Hence, in addition to security measures stated across other chapters, the Data Center needs special consideration of IT security, as under.

P-11.2 Location of the Data Centre should have maximum safety from geographical threats like earthquake, flood, fire, hurricane, tsunami, etc. and socio-political threats like unrest, agitation, riots, civil commotion etc.

P-11.3 The site should have a minimal social and proximity hazards like busy street with traffic throb, humming machinery, magnetic field, effervescent fumes, etc.

P-11.4 Wherever any such adversities are inevitable or they crop up in future, the suitable mitigating action should be taken, like say wooden platforms to absorb the shocks, false ceiling to absorb the heat, metal grid/foil shield for electro-magnetic field/high frequency waves, etc.

P-11.5 There must be well conceived and tested plans for easy and swift evacuation of the workforce at Data Centre, should the emergency situation arise. Such plans must be known and practiced by one and all at Data Centre.

P-11.6 There will be multi-tier security architecture for Data Centre and the security should strengthen towards central core part.

P-11.7 Entry to the Data Centre will be restricted to the authorized personnel only and the authority for the decision will be the Data Centre Head.

P-11.8 Such entry will be based on proximity cards and a traffic log will be maintained automatically by the system as also manually in the register by the watchman. This log will be scrupulously looked into at least once a week.

P-11.9 Any IT devices like computer, storage media etc. that enters or leaves the Data Centre shall be with prior permission of the Data Centre Head and it will be properly monitored and logged.

P-11.10 Computing devices like laptop, PDA, pen drive etc. and cell phones will not be allowed to be carried inside the core area of the Data Centre, that houses various servers and networking equipments.

P-11.11 All the hardware and networking equipment will be properly configured and these settings will be periodically reviewed by the respective in-charge.

P-11.12 Servers and high end networking equipments at Data Centre shall be equipped with resilient features like hot swapping, automatic fallback, etc. to ensure high availability of the computing resources to the branches for Jhalawar Kendriya Sahkari Banking functions.

P-11.13 Wireless LAN is discouraged at Data Centre unless the security aspects of this technology reach reasonable maturity. In case it has to be installed for certain business considerations, it should be tested for penetration immediately on installation and also regularly at quarterly intervals.

P-11.14 Data Centre should have arrangements for alternate sources of communication, power and other necessary utilities.

P-11.15 Branch Jhalawar Kendriya Sahkari Banking software shall be isolated – logically and as far as possible physically also – from the other software deployed at the Data Centre, to ensure smooth and undisturbed Jhalawar Kendriya Sahkari Banking operations.

P-11.16 Each version of the Jhalawar Kendriya Sahkari Banking application shall be thoroughly tested till satisfaction of Jhalawar Kendriya Sahkari Bank. This will be done by the test group at Data Centre in an isolated and frozen environment and test problems, if any, should be suitably escalated, jointly discussed and resolved with the developer, before the software is put to live use.

P-11.17 Barring the user-definable customization modules for validation of data inputs, workflows and reports, with addition in data base structures for the same, if any, no other part of core Jhalawar Kendriya Sahkari Banking software shall be modified at the Data Centre itself. These modifications will be neatly documented for audit, future use and will be tallied with logs, if possible.

P-11.18 Various techniques will be used for backups like mirroring, RAID, automated systems, off-site backup, etc. The backup will be suitably restored at the Disaster Recovery site to ensure availability of updated data.

P-11.19 For each person working at Data Centre, another appropriate person may be identified as substitute in cases of need. This should be mandatory for mission critical operations. The skill set of these two persons should be kept in as synchronized to each other, as possible.

P-11.20 Vertical rungs of organizational ladder at Data Centre should have adequate functional flexibility for upward and downward mobility to ensure smooth working.

P-11.21 Duties of system administration, network administration, security administration and database administration shall be segregated at Data Centre.

P-11.22 Business Continuity Plan for the Data Centre shall be periodically reviewed with frequency of an at least once a year and shall be suitably refined, if need be.

P-11.23 Disaster Recovery Site (DRS) shall be tested initially in parts and subsequently in full after its stabilization.

P-11.24 Jobs at Data Centre should be rotated at least once in a year.

P-11.25 Infrastructure and operations at Data Centre will be periodically inspected to pinpoint the single point of potential failure, if any. Such point will be supplemented with an adequate compensating control.

P-11.26 Data Centre will not initiate any Jhalawar Kendriya Sahkari Banking business transaction except the en mass automated activities like interest calculation that may be carried out on behalf of the branches.

P-11.27 When the modifications in the raw database are inevitable due to certain reasons (like some limitation of the application software in tackling the rare business scenario), a two-fold process should be taken up

Prior approval (at least over phone, if the sanctioning authority is out of station / distant away) to such an update will be taken essentially from the Head of IT at C.O. by fully documenting the details of the case.

Actual database update operation shall be performed under dual control. (Documentation with two officers authenticating the change in their presence)

P-11.28 Data Centre will undergo security audit as per the frequency decided by the Jhalawar Kendriya Sahkari Bank. No two consecutive audits shall be done by one and the same team.

P-11.29 Workforce at Data Centre should undertake Control Self Assessment (CSA) at least once in a year.

P-11.30 In case of any security incident at Data Centre, the Data Centre Head shall directly address the incident to the Head of IT at C.O., who will be the competent authority to decide the matter.

IT Asset Inventory

Policy

Inventory of all hardware, network equipments and software will be maintained to provide control over its availability.

Procedures

P-12.1 Inventory of all hardware and software media will be maintained. Based on its nature category for Hardware, Network Equipment, Peripherals, Software Media, etc. will be defined.
P-12. 2 Inventory of all purchased or leased items will be maintained.
P-12. 3 Inventory of all software media not limited to original software, backup of software configuration, configuration backup, will be maintained.
P-12. 4 Each IT asset will be identified with a unique numbering that will be written on the IT asset as well in the inventory register.

Information System Audit

IS Audit is a process of collection and evaluation of evidences for determining whether the information system safeguards assets, maintains data integrity, achieves organizational goals effectively and efficiently in view of the IT policy of the bank. IS Audit is a planned process shall be carried out on test basis. The IS Audit ensures that IT system of the bank is available for business at all times, the system is highly secure and protected against all threats, losses and disasters. It also ensure that the bank's IT environment is accessible to only authorized users and not to anyone else, the information provided is accurate, reliable and timely available. The bank management shall ensure that no unauthorized modification of data or software is made. IS Audit informs envisages physical and environmental review, administrative review, application software review, network security review, business continuity review, data integrity review etc.

IS Audit will be conducted by a qualified audit form or by a team of competent IS audit personnel on annual basis covering all critically important branches (in terms of nature and volume of business) and functions at bank's HO/Controlling offices. NABARD guidelines circulated vide Circular no.33/DOS-01/2015 dated 25.2.2015 shall be complied with.

Periodicity of IS Audit

The IS Audit shall be preferably undertaken prior to statutory audit so that the IS Audit reports are available to the statutory auditors well in time for examination and incorporating comments.

Review of IS Audit by Bank's Board

The IS Audit report shall be place before the bank's Board of Directors and Audit Committee of the Board to ensure that the guidelines are implemented with modifications that suit the local conditions and level of computerization in the bank.

Broad rules for Information System (IS) Audit

Information System Audit is a series of tests that must be conducted periodically or for special purpose to ensure that adequate controls are in place over the Information System. Information System Audit is not a Financial Statement Audit and it does not test financial statement data for determining existence, completeness, rights and obligations, valuation or allocation and presentation and disclosure.

1. The purpose of IS Audit is to review and provide feedback, assurance and suggestions on the concerns of the management with regard to integrity and effectiveness of systems and control. These concerns can be grouped under three areas which are related to the systems :

   1.1 **Availability**: Whether the information systems on which the business is heavily dependent is available for the business at all times when required. Are the systems well protected against all types of losses and disasters High availability systems aim to remain available at all times preventing service disruptions due to power outage, hardware failures and system upgrades.

   1.2 **Confidentiality**: Whether the information in the systems is disclosed only to those who is authorized to see and use it and not to anyone else.

   1.3 **Integrity**: Whether the information provided by the system is always accurate, reliable and is timely. What measures are available to ensure that no unauthorized modification can be made to the data or the software in the system

The IS audit aims to provide reasonable assurances on test basis regarding the adequacy of the controls used in the governance over IS resources and covers all the major and common types of audit, viz. Systems Audit, Application audits, Compliance audits, Security audits, Performance audits, etc. 5

2. Banks shall put in place a mechanism for conducting IS audit on perpetual basis. IS audit shall be conducted by a qualified auditor/ audit firm. Banks may constitute an IS audit cell as part of its Inspection and Audit Department to carry out IS audit in branches / offices having computerized operations. However, bank, may also create a dedicated group of persons, who, when required, can perform functions of an IS Auditor. The overall control and supervision of these IS Audit Cells should be vested in the Audit Committees.

3. A team of competent and motivated IS personnel may be developed. It is beneficial to have a collective development system consisting of many persons instead of a few, in order to take care of a possible exodus of key personnel. IS auditors' technical knowledge should be augmented on a continuing basis through their deputation to seminars / conferences, supply of technical periodicals and books etc.

4. Duties of system programmer/designer should not be assigned to persons operating the system and there should be separate persons dedicated to system programming/design. System person would only make modifications / improvements to programs and the operating persons would only use such programs without having the right to make any modifications.

5. The loopholes and major factors which lead to security violations in computers i.e. inadequate or incomplete system design, programming errors, weak or inadequate logical access controls, absent or poorly designed procedural controls, ineffective employee supervision and management controls shall be plugged by

   (i) strengthening physical, logical and procedural access to system;

   (ii) introducing standards for quality assurance and periodically testing and checking them; and

   (iii) screening employees prior to induction into IS application areas and keeping a watch on their behavioral pattern.

6. The system development methodology, programming and documentation standards to be followed by the bank, shall be formally declared. In its the absence quality of system maintenance/improvement might suffer. IS auditors should verify compliance in this regard.

7. Contingency plans/procedures in case of failure of system should be introduced/tested at periodic intervals. IS auditor should put such contingency plan under test during the audit for evaluating the effectiveness of such plans.
8. A manual of instructions shall be available for auditors and it should be updated periodically to keep in tune with latest developments in its area of operations and in its policies and procedures.
9. An appropriate control measure should be devised and documented to protect the computer system from attacks of unscrupulous elements. Before introducing an IS application in place of certain manual procedures, parallel run of both the systems should be done for a reasonable period to ensure that all aspects of security, reliability and accessibility of data are ensured in the IS application.
10. In order to ensure that the IS applications have resulted in a consistent and reliable system for inputting of data, processing and generation of output, various tests to identify erroneous processing, to assess the quality of data, to identify inconsistent data and to compare data with physical forms should be introduced.
11. While engaging outside computer agencies, bank shall ensure to incorporate the "clause of visitorial rights" in the contract, so as to have the right to inspect the process of application and also ensure the security of the data / Data Centre / Disaster Recovery Centre / inputs given to such outside agencies. Agreement with vendor should take care of probable data leakage.
12. Entire domain of IS activities (from policy to implementation) should be brought under scrutiny of Inspection and Audit Department. Financial outlay as well as activities to be performed by IS department should be reviewed by senior management at periodic intervals.
13. The information systems auditor is to provide a report in an appropriate form, upon completion of audit work. The audit report is to state the scope, objectives, period of coverage and the nature and extent of the audit work performed. The report is to state the findings, conclusions and recommendations with respect to improvement in data integrity, system effectiveness and system efficiency.

Check list for the guidance of Auditor carrying out IS audit

I. Segregation of Duties

I.A. Segregation of duties between the data processing function and users.

a. The organizational structure shall provide for separation of functions between:
    i. Transaction initiation & authorization
    ii. Console operations and data-entry
    iii. Program team and Custody of System Documentation (including programs), confidential data, etc.

b. The Data Bank Administrator (DBA)/IS manager shall reports to higher authorities about day-to-day as well as non-routine activities.

c. The data processing personnel shall be restricted from having asset custodianship functions, and access to assets, particularly liquid assets.

I.B. Segregation of the duties within the IS functions

a. A current organization chart which defines the organizational structure within IS department/EDP Department shall be defined

b. There shall be current job descriptions for all personnel associated with IS department/EDP Department.

c. The new employees shall be provided with orientation upon recruitment.

d. IS department/EDP Department employees shall be provided with formal and on-the-job training to maintain knowledge, skills and ability in Information Technology and control-requirements.

e. There shall be a separation between Data Base Administration and other data processing functions.

I.C. Precautions regarding personnel involved in IS functions:

a. Employees who constitute a potential threat shall be transferred or suspended immediately.

b. References shall be verified before an employee is recruited.

c. The IS personnel (including DBA) is required to take regular vacations, and are their duties reassigned during the vacation period

II. Access Controls

II.A. Access controls: The access to the main processor (i.e. system-console or server) shall be adequately controlled.

a. The computer room shall have adequate physical barriers to prevent unauthorized access to the system console / server.

b. Combination locks, security badges or other means will be used to restrict access to the computer server room, back-up storage library and documentation library.

c. Combination locks, security badges or other devices shall be changed periodically.

d. Detective equipment have to be installed to monitor access to the computer server rooms, (or e.g. cameras with time and date stamp in case of ATM-Unit).

e. The location of off-line storage of data, transaction journals and critical reports should be safeguarded against unauthorized access.

II.B. Access controls: Adequate procedures for access to programs and data including Data Centre/Disaster Recovery Centre and primarily controlled through passwords.

a. Password administration facilities in Operating System (OS) and in Application packages are in vogue.

b. A security package is in use, or any other security facilities in O.S. and App. Packages could be explored

c. Suitable security software shall be installed and updated regularly in all systems for protecting software systems against virus, spyware, spamware and other malicious programs.

d. Various levels of passwords are to be established for different transaction types, files and programs.

e. Various levels of passwords are to be required based on the usability, confidentiality and significance of information

f. Passwords shall be periodically changed. The duration of how often passwords are changed shall be defined.

g. All modifications to authorization tables and access privileges shall be recorded and reviewed.

h. All Systems/Database logs are to be validated by the Solution/Service provider at periodical intervals

i. Log-in IDs of retired/terminated employees are immediately disabled on the system.

j. Users shall be prohibited from selecting passwords that contain their names, or the passwords, which are very easy to guess.

k. If the DBA/password administrator assigns passwords first time, the delivery procedures have to be appropriate to assure that an employee's password is not intercepted.

l. Employee shall be prompted to change the password immediately after he receives from the DBA.

IIC. Access controls: Adequate procedures to access programs and data files that is primarily controlled through physical restrictions in terminals.

a. The layout of the area where terminals are located should prevent unauthorized access to equipment.

b. The location of terminals used for either data entry or inquiry must restrict access to authorized personnel when the system is in operation.

II D. Access controls for proper control of the programming activities.

a. The procedures and system - mechanisms should prevent programmers from accessing production data, object programs and other automated procedures during the testing and debugging process.

b. Programmers should be required to work on a separate computer system (i.e. other than production system).

c. All live data is to be removed from the computer system and secured in a separate library at the time software or hardware maintenance activities take place.

d. The production software (i.e. programs in use) should be protected from unauthorized access (i.e. use of a restricted facilities).

e. All testing activity should be restricted to non-production programs and data

f. The procedures used FOR INCORPORATING NEW OR ALTERED PROGRAMS IN PRODUCTION SYSTEMS should prevent unauthorized access to other programs.

II.E. Access controls: system-activity to be appropriately monitored.

a. The computer system should maintain a log of access activity.

b. Invalid access attempts should be reported to, and investigated by management, DBA, and Computer Auditors.

c. The system should be capable of distinguishing activity source by terminal identification.

d. The system should be capable of identifying authorized individuals by multi-level passwords.

e. All entries by personnel restricted or secured areas should be recorded.

II.F. Access controls: hardware and software maintenance should be properly monitored and controlled.

1. Supervisory activities should ensure that all hardware and software-maintenance is:

    a. Identified

    b. Authorized

    c. Recorded

    d. Reviewed

    e. Monitored

II.G. Access controls: the operating system should be properly controlled.

a. The operating system options / configuration settings should be properly documented.

b. The operating system shall be free of extensive modifications.

c. The modifications in operating system configuration-settings shall be subject to the same controls as application programs.

d. The data processing department shall have a system-software programmer on staff.

e. The patches/ upgrades / updates must be applied regularly on operating systems and other system applications.

II.H. Access controls: Distribution of Reports

a. The procedures for receipt and distribution of computer-outputs must ensure that access to information is authorized.

b. A report distribution list should be used, for this purpose.

c. The waste disposal procedures should include the destruction of obsolete reports, which contain sensitive data.

II.I. Access controls: Access to blank cheques, demand drafts and other critical documents must be controlled

a. These documents may be issued (internally to the concerned employee/s) on the basis of run schedules only.

b. These documents are kept locked in a secure location when unattended

c. The records of supply of these forms shall be maintained

d. The records of ACCESS TO supplies of these forms have to be maintained

e. These documents should be periodically inventoried

f. The documents may be pre-printed.

g. The documents when pre-numbered or sequentially numbered should be accounted for.

II.J.Access controls: Other access controls in place in the following areas

a. All computer language-compilers should be removed from the production system, (and at the location of software development site, protected from unauthorized access).

b. If the computer system uses an interpreter of the language, there have to be adequate measures been taken to prevent the illegal interrupt of program execution or alteration of program logic by computer operators.

c. Report-generation packages should be secured from the update capabilities (especially from modifying the contents of the reports generated).

d. The reports generated should clearly identify their source.

e. The availability of utilities, which can be used to alter or copy data and programs should be restricted and controlled

III. Authorization

III.A. **Authorization:** The bank’s top management/Board shall authorize the following IS-related functions

a. IS Personnel Policy

b. Hardware Policy

c. Software Policy

d. Software Development Policy
e. Programming Methodology
f. IS Security Policy
g. Documentation Policy
h. Information Policy
i. Priorities of IS-related activities
j. Major system / design /equipment changes
k. Manpower allocations by project
l. Procedures for security and control measures
m. Research and Development studies
n. IS budgets
o. IS long-range plans

III.B. Authorization: only authorized transactions to be processed, and unauthorized transactions (if any) to be identified

a. Clerks/computer-operators may be provided an approval-form to assure authorization (in addition to on-line authorization), in order to process the transactions
b. The computer system shall verify authorization for transactions entered on-line, through terminal identification (i.e. a data-entry terminal cannot be used simultaneously as authorization terminal).
c. Individuals shall be held accountable for all transaction-activities through the use of transaction – logs.
d. The transaction logs should contain the log in-id, the source (i.e. terminal #), Voucher #, Date & time of transactional for ALL the transactions during on-line data-entry.
e. Are permanent records of ALL the live programs and data on the computer system (in the following areas), shall be maintained by System Administrator &Branch Manager.
    i. Production (i.e. live) files and directories
    ii. Production program libraries
    iii. Production environment parameter settings (e.g. O.S. and DBMS configuration settings)

III.C. Authorization: written standards to be developed/prepared to provide management's general and specific authorization for various IS-related activities

a. A written manual of systems and procedures should be available for all computer operations, and it should provide a definition and explanation of management's general and specific authorization to process transactions.

b. There have to be written standards for:

   i. Hardware selection

   ii. System Software selection

   iii. Application package selection

   iv. Network component selection

   v. System design and development

   vi. Programming standards

   vii. Testing

   viii. Program approval standards

   ix. Implementation (including procedures for putting a program/system into production)

   x. Hardware and especially Software Change Management Procedures

III.D. Authorization: The system development should be properly controlled

a. A formal System Development approach should be used

b. Management should make a clear distinction between production (i.e. live) and development programs

c. "Prototyping" may be done

d. The procedures for system design, including the acquisition of software packages must have active participation by representatives of users, accounting, internal audit, and computer auditors (I.S. auditors), as appropriate

e. Each system must have have a written (in detail) specification, which are reviewed and approved by management, and applicable users before preparation of the detailed systems design specifications to assure implementation of an acceptable quality standards

III.E. Authorization: The new systems should be adequately tested

a. The software-testing must be a joint effort of programmers, system developers, computer (I.S.) - auditors, and users

b. The system testing must include testing of both, the manual and computerized phases of the system

c. Test data must be developed to specifically test the functioning of programmed control procedures.

d. During parallel testing, consideration should be given to whether errors exist in the populated data, to test programmed controls

e. A documentation of system tests (data and results) must be retained for future use, which will be required in case of later system modifications

f. The test results must be reviewed and approved by user / management personnel before authorizing the transfer of programs into the live environment

g. The final testing procedures should provide user, management, IS-staff and IS-audit personnel with a clear identification of the program version used to perform the test

h. The programmers shall be prohibited from using live data files to test programs.

III.F. Authorization: System conversion to be adequately planned and controlled

a. Formal, written conversion procedures to be prepared

b. Formal approval by system development steering - committee / bank's management and IS auditor to be obtained, of IS related activities including a review of changes from original design specifications, review of system test results, review of input and output controls, and review of documentation prior to putting a new system into production

c. These written conversion procedures to be approved by bank management, internal audit, IS auditing, user departments and accounting personnel as appropriate

d. All master file / table and transaction file / table conversions must be controlled to prevent unauthorized changes, to provide accurate and complete results, and to ensure data integrity

e. Program transfer - procedures to ensure that only those programs, which were used for the final test, are transferred to the live environment

f. The control totals such as record counts and hash total shall be established to allow reconciliation of converted files to the original manual or computer files

g. Critical matter files / tables to be printed before and after conversion (e.g. deposits file, payroll master file / table, central information table / file, etc.)

h. Someone without incompatible duties should compare the before and after details of these critical matter files / tables

III.G. Authorization: program changes must be authorized

a. Policies and procedures for initiating changes to programs and other forms of processing logic to be ensured that management authorizes all changes

b. Policies, procedures and mechanisms to ensure that personnel responsible for application program perform no changes to the operating system configuration

c. A log should be maintained of all changes requested that identify the person initiating the change, the date initiated and the date implemented

d. This log should also identify the specific program (s) and / or operating procedures affected by the change

III.H. Authorization: program changes to be monitored and controlled

a. Procedures ensure that all changes to the system are documented

b. Program modifications made ONLY TO COPIES OF current production programs rather than the programs themselves

c. A responsible official INDEPENDENT OF PROGRAM to authorize operations personnel to put a modified program into production

d. Source programs to be supplied when program changes are authorized for putting into live operation

e. The following documentation to be obtained/prepared before and after each change, and retained as a permanent record

    i. Files / directories in the system

    ii. Production library directories

    iii. Program source listings

    iv. Operation procedures' listings

    v. Systems flowcharts

    vi. Data flow diagrams

    vii. Entity Relationship (ER) diagrams

f. Operations' procedures should be updated to reflect system changes

g. System administrators of all transfers to production libraries (i.e. live environment) shall maintain logs

h. If patching techniques are used:

    i. They shall be allowed only in emergencies

    ii. They shall be allowed only after supervisory approval

    iii. Records of patches to be maintained, including appropriate approvals, records of the instructions / routines altered, the name of the person making the changes and the reason for the changes

IV. Supervision and Review

IV.A. Supervision and review: The IS related activities shall be subject to review by management

a. Management should be knowledgeable about the activities performed by the computer system and the methods used for operation and maintenance of the system

b. Logs of computer processing and balancing activities should be available, and reviewed by Management at least on half-yearly basis.

c. Logs form the basis for preparation of performance statistics to be reviewed by management

d. Logs forms the basis for charging computer expenses to user departments, (if applicable)

e. The system log file / table properly shall be controlled to prevent unauthorized changes

f. All reports of reprocessing activity to be retained, reviewed by supervisory personnel and is computer time accounted for

g. Computer processing to be scheduled, either manually or through automated techniques, and regularly compared to machine utilization reports and / or console logs

h. The processing schedule to include periodic (i.e. daily, fortnightly, month-end, quarterly, six-monthly, yearly, exceptional etc.) processing-requirements

i. Significant variations from scheduled processing shall be investigated

IV.B. Supervision and review: The management to periodically review access - authorization

a. Authorization levels for terminal users and points of transaction / operation organization to be periodically reviewed

b. Supervisory or managerial personnel shall routinely review the logs and reports of invalid access attempts

IV.C. Supervision and review: Computer operations to be well documented and organized in an orderly fashion

a. The computer operations staff (including DBAs / System Administrators, and computer auditors) shall be adequately trained to the extent necessary to perform all their tasks in a systematic manner (without relying upon external personnel)

b. Computer processes to detect or prevent the initiation of processing steps, which are OUT OF SEQUENCE

c. Hardware maintenance boundaries to be contractually defined with each vendor when the bank (or even a branch / office within a bank) uses hardware from more than one manufacture

d. A record of all Hardware problems (including UPS) to be properly maintained in a register.

e. A record of all Software problems to be properly maintained in a register

f. Preventive maintenance to be routinely performed at a frequent interval.

g. A record of such maintenance to be prepared and reviewed

h. The use of off-line data files for processing shall be controlled through verification by the system, before the processing is initiated

IV.D. Supervision and review: Management has to establish documentation standards to allow for maintenance and supervision of IS-related activities in the following areas:

a. Information Systems setup documentation (at each location)

b. Systems documentation

c. Programs documentation

d. Operations documentation

e. User documentation (e.g. user profile and the kind of operations he is allowed to perform)

f. Supervisors to review "Users" and "Technical" manuals to make sure that prescribed documentation standards are adhered to

g. "Documentation standards" and "change procedures" to be adequate to ensure that documentation is maintained in a correct and consistent manner

IV.E. Supervision and review: Adequate and up-to-date system-documentation to exist (for every system) including the following:

a. Systems narrative

b. Systems flowcharts

c. Broad input-design

d. Broad Database design

e. Broad (context-level) DFDs i.e. Data Flow Diagrams

f. Data element definitions

g. Codes Design

h. Dialogue Design

i. Broad Procedure-Design

j. Held Design

k. Broad Output Design (Report and Screen Design)

l. Data capture procedures

m. Backup and recovery procedures

n. System changes

IV.F. Supervision and review: Adequate and up-to-date documentation shall exist including the following:

a. Detailed System Flowcharts

b. Narrative description of each major program module, subsystem

c. In-detail program-flowcharts

d. In-detail DFDs (Data Flow Diagrams)

e. Decision tables

f. In-detail database design

g. In-detail ER diagrams

h. List of constants, codes and tables used

i. Source program listing

- Operating System (OS) Commands listings
- Specimen vouchers
- Specimen data-entry (and other interface) screens
- Specimen reports
- Program changes
- Changes in ANY COMPONENT of the system

IV.G. Supervision and review: Computer jobs streams to be supported by computer set-up and run instructions including:

a. Set-up instructions and device assignments

b. Identity of input and output data tables/files

c. Parameters of Job Control Language /OS Commands

d. Normal console/server-messages for each run

e. List of error and halt messages, probable causes, programmed and machines halts, and required action

f. Restart and recovery procedures

g. Estimated run times and maximum run time (for every major job /major task)

h. Form (and distribution) of printed and other outputs

i. End of job instructions

j. Output destination and retention instructions

IV.H. Supervision and review: Procedures for input and output to be documented

a. Input procedures need to be documented to describe all tasks necessary for the control of transactions processed by the system including:

   i. Input receipt

   ii. Data entry

   iii. Error correction

   iv. Source document control

   v. Permanent record retention

b. Procedures to be documented for the generation, verification and distribution of computer output including:

   i. Output reports generation

   ii. Report balancing and reconciliation

   iii. Report distribution

   iv. System inquiries

c. Control totals need to be produced by the system to allow balancing with input control totals including:

   i. Batch number

   ii. Amount totals of significant fields

   iii. Hash totals of significant fields

   iv. Transaction or record counts

   v. Ending number of master file records

   vi. Total number of master file / table records

V. Security and recovery

V.A. Security and recovery: The potential risk of events, which could cause short-term or sustained loss of computer-processing capability have to be identified

a. The maximum time period, for which loss of computer processing could be tolerated without serious disruption to the business has to be identified (separately for every business-operation based on nature and criticality of that business operation)

b. The effect of loss at differing times i.e. start of day, peak business-hours time, end of week, end of month, end of year etc.) have to be addressed

c. The effects of daily operating practices, customer reaction, and exposure to loss have to be considered

d. The effect of loss of individual components of the system (Hardware components, network components, system and application Software components, data, documentation, people etc.) have to be isolated

V.B. Security and recovery: Information Systems activities related insurance coverage have to be considered for the following risks:

a. Equipment destruction

b. Program or software destruction

c. Loss of data

d. Business interruption

e. Errors of omissions

f. Fidelity insurance on IS personnel

g. Payment for use of alternative equipment

h. Annual management review and approval of IS activities related insurance coverage

V.C. Security and recovery: The plans and procedures must exist to prevent a short-term or partial failure in a controlled manner

a. The environment for the computer systems shall conform to manufacturer's specifications for electrical, humidity, temperature and air particle tolerance

b. The physical location of computer equipment to discourage access or interruption by unauthorized personnel and reduce vulnerability to environmental effects and natural disasters

c. The on-premises backup-storage area should provide reasonable protection against accidental damage or destruction of data, programs and documentation

d. The bank shall have written policies and procedures for backup and recovery of all data and programs stored on magnetic media, to assure sufficient backup exists to restore them if they are destroyed

V.D. The plans and procedures shall exist to recover from a short-term or partial system failure in a controlled manner

a. Procedures must exist for recovery in an orderly manner in the event of processing interruptions resulting from such occurrences as equipment malfunction, power fluctuations, software error or loss of on-line data

b. Procedure shall be there for continuation of processing in the absence of key individuals (IS persons) within the branch/office

c. Programs, which have backup data, should be included in the routinely run application software, so that the backup procedure will not be a DBA's or operator's choice

d. At least one current copy of the supervisory and application program library need to be maintained in the nearby magnetic-storage-library, as immediate backup

e. An error-recovery procedures should exist for short-term failure tested periodically to ensure control of the process

f. Computer operators' duties to be rotated periodically, to have internal controls, and also to ensure the availability of trained backup staff

g. The "Maker-Checker" principle to be used in Software development activities also

V.E. Security and recovery: are backup procedures adequate

a. Current copies of the following should be maintained off-site :

i. Operating systems

ii. Source programs

iii. Runtime (executable) codes

iv. Master data

v. Transaction data necessary for recovery

vi. Program documentation

vii. Operating instructions

viii. Critical forms and supplies

ix. Disaster recovery plan

x. System documentation

b. When "backup copies" of programs are used, they should be duplicated before being put into production

c. When backup copies of master or transaction data are used, they need to be duplicated before being put into production

d. Restoration / recovery procedures need to be tested periodically, after having secured backup copies of all data, software, documentation and transaction sources

V.F. Security and recovery: are the arrangements with vendors adequate

a. Vendors to be responsible for reliable hardware and software support to avoid the possibility of processing interruption due to lack of support

b. Remedial equipment - maintenance arrangements to be provided for response to problems in sufficient time to prevent business disruption

c. The average response time after registering the complaint to be defined

d. The equipment maintenance vendor to maintain an inventory of replacement components (which are frequently required for local service)

V.G. Security and recovery: The disaster recovery planning need to be adequate

- There need to be a detailed disaster recovery planning explaining procedures and steps necessary for recovery after the disaster
- A copy of the plan to be stored off premises or in a location where it would not be destroyed in the event of a disaster
- Backup alternatives may been considered and deployed (i.e. hot site, cold site, warm site, reciprocal arrangements, etc.)
- Alternative computer equipment arrangements should be tested periodically to ensure that the plan functions
- The disaster recovery plan need to been tested

V.H. Security and recovery: Recovery - considerations should be adequate

a. Documented operating procedures should permit continuation of computer processing in the event of permanent loss of key operations personnel

b. The documentation of the system should permit maintenance by alternate support personnel in the event of loss of key programmers

c. The Disaster Recovery Plan (DRP) should include the provision for continuation of business operations in the event of any (minor or major) disaster

d. The bank (i.e. every computerized branch and office) in compliance with the regulatory / statutory requirements, with respect to retention of data should generate reports which is in the machine-readable form

Scope of IS Audit

The indicative scope of IS Audit is given below :

- Alignment of IT strategy with Business strategy
- IT Governance related processes
- Long term IT strategy and Short term IT plans
- Information security governance, effectiveness of implementation of security policies and processes
- IT Architecture
  - Acquisition and Implementation of Packaged software

    - Requirement Identification and Analysis
    - Product and Vendor selection criteria
    - Vendor selection process
    - Contracts
    - Implementation
    - Post Implementation Issues
    - Development of software - In-house and Out-sourced
    - Audit framework for software developed in house, if any
- Software Audit process
    - o Audit at Program level
    - o Audit at Application level
    - o Audit at Organizational level
- Audit framework for software outsourcing
- Operating Systems Controls

> Adherence to licensing requirements

> Version maintenance and application of patches

> Network Security

> User Account Management

> Logical Access Controls

<u>Adoption of Board Approved Information Security Policy and its review</u>

The Information Security Policy is adopted with the approval of the bank's board appropriate to the level of computerization/CBS system deployed by the bank. The policy will be reviewed at regular intervals in tune with industry best practices and as per guidelines issued by RBI/NABARD from time to time.