Sl.N0.	**System Audit Questionnaire**	
	Background	
1	What is the information technology environment?	
2	Give a brief description of the equipment.	
3	Has a map of the installation been prepared? Otherwise, obtain one.	
4	What are the operating systems in use?	
5	What are the communications systems in use?	
6	What are the various applications which have been computerized?	
	organisation	
1	Prepare or obtain an organizational chart of information technology department.	
2	Determine job title, job descriptions and names of the persons in IT department.	
3	Is there a segregation of duties such as: a. Functions and duties of systems design, programming and data administration are separate from computer operations;	
	b. Programmers do not operate the computer or regulate processing runs;	
	c. Operators have access only to such data and programs as is necessary for performing their assigned tasks;	
	d. Personnel in data processing department are not performing any duties relating to organizing transactions or making changes to master files.	
4	Are the duties of computer operators periodically related?	
5	Are there well-documented operating procedures?	
6	Are the operating functions being properly supervised according to programmed operating procedures?	
	Control Functions	
1	Are there persons specifically given the responsibility for performing the control function in the information technology department?	
2	Do there duties include control over receipt of input data and recording of control information?	
3	Is there control over distribution of output?	

4	Is there control over errors to insure that they are reported, corrected and reprocessed? Is review of appropriate logs of error detection and control regularly done?	
5	Are master file changes or changes to data authorised in writing by appropriate personnel in the department initiating that changes?	
6	Is there any written communication made available to the department initiating the changes informing the IT department of the changes actually made?	
	Management Practices	
1	Is there a corporate security policy?	
2	Are there any procedure regarding physical security covering the following features: a. Office building;	
	b. Entry to computer centre;	
	c. Access to client's computer systems;	
	d. Access to server systems;	
	e. Working after office hours;	
	f. Procedures for the prevention and protection.	
	Organization Controls	
1	Are there clear segregating of duties within the IT department?	
2	Are there separations of duties between IT department and user departments?	
3	What are the procedures regarding access to data within the computer system?	
4	Password management: a. Access to corporate data base;	
	b. Access to application programs.	
	Systems Development Methodology	
1	Are there any standards for systems development?	
2	Have the standards been implemented, and if so, to what extent?	
	Program Change Management	
1	Are there standard procedures laid down for changes to existing programs?	
2	Do they cover the following: a. Authorization for change;	

	b. Independent testing;	
	c. Compiling and adding to the library of programs by a person independent of the programmer.	
3	Are the standard procedures being implemented?	
	Program Library Maintenance	
1	Are there well laid out procedures for maintaining computer library?	
	Business Continuity Planning	
1	Is there a well-documented business continuity plan?	
2	Has it been well-documented and updated?	
3	Does it contain procedures regarding:	
4	Data backup	
5	Backup of hardware, software and communication infrastructure.	
6	Are there provisions for use of alternative facilities in the event of fire or other long interruptions?	
7	Is there adequate insurance cover for various likely disasters?	
8	Is date processing personal covered by fidelity insurance?	
	Environmental Controls	
1	Whether the location of computer installation is safe from potential hazards such as water seepage, fire, flood etc.? If not, what precautions have been taken to overcome such problems?	
2	Whether ATM/Server Room is clean and the environment is dust free.	
3	Whether the electrical and data cabling has been done in a structured manner and is not exposed except at the terminal point? Comment on the status of cabling and hazards, if any.	
4	Whether power supply to IT systems is backed up though UPS and is not being used for any other purpose except for the minimal support light?	
5	Earth to neutral voltage is 0-2 volts, which should be got tested during the course of audit (incumbent to arrange for the same). Comment on the deviation, if any.	
6	Whether the server, if any, is placed in a separate partition/ room and telecommunication line(s) is/are available in the server room/partition?	
7	Whether air conditioning, ventilation and humidity control procedures are in place for Servers/ critical equipments/ATM / UPS etc.	

8	Whether the Switch/hub is placed in a mounting rack under lock and key?	
9	Whether gas-based fire extinguishers are available and the same are valid and in working condition?	
	Physical controls:	
1	Whether the server/most critical equipments such as PC for backup/Switches/Routers are located in least accessible area and the access is restricted to authorized persons only?	
2	Whether all the IT equipments have been allocated and marked with unique number and are in consonance with the inventory register.	
3	Whether all the configuration details have been mentioned in the Inventory Management Register However, if the record is maintained in PC, print out of the same should be pasted in the register and updated regularly.	
4	Whether the access to IT installations is restricted to authorized persons only. Whether access violations are properly recorded and appropriate actions taken the regainst.	
5	Whether all PCs/Printers are regularly cleaned and covered when not in use?	
	Logical Controls:	
1	Whether all the PCs are protected by boot password?	
2	Whether all the users have been created with written permission of the Incumbent/Head of the Department?	
3	Whether any generic user account name has been created except reserved users account for Operating System, RDBMS and Application Packages?	
4	Whether sensitive user IDs (e.g. root, RDBMS, DBA etc) and passwords are maintained as per HO guidelines and the prescribed procedures are being complied with such as : a. Whether passwords are kept in a dual custody in sealed cover.	

	b. If opened, whether the password has been changed and again kept in sealed cover.	
5	Check whether access rights for system files, executable files, data files and parameter files etc. are given on need-to-know/ need–to-do basis.	
6	Whether proper record is maintained in respect of Creation/ Deletion of USER IDs in the user maintenance register on specific approval of Incumbent In charge or Departmental Head? Verify if such approval is in place in respect of the entire active user IDs.	
7	Whether Enabling and Disabling of User ID s is done daily prior to start of the work as per daily arrangement register and active user ID s in the system are in agreement with the register? Report violations, if any.	
8	Whether USER IDs are unique?	
9	Whether proper record is maintained for the password of other users changed by the DBA/System Administrator in the register and same carries approval of the Incumbent? Comment on the number of Data Base Administrators/System administrators active at a time.	
10	Whether the control on maximum number of invalid logon attempts to three has been specified properly in the system.	
11	Whether automatic logout in case of unattended terminals is available on windows/UNIX environment? Specify the time set.	
12	Whether the parameter to control maximum validity period of password is set to 15 days. If not, what is the validity period?	
13	Whether declaration for maintaining confidentiality of password is held for all the users?	

	Application Systems Controls:	
1	Give package-wise details of bugs/deficiencies reported along with the steps taken for their removal. Whether these are recorded in Software Problem Register? Whether compensatory controls are put in place to ensure correct and valid output? (Attach separate sheet, if required)	
2	If source code is available: a. Whether there is adequate separation between the development and production environment.	
	b. Review the adequacy of access controls to source code.	
	c. Whether the custody of source code is with the authorized official (s)?	
	d. Whether proper handing over procedures is being adopted in the event of transfer/change of authorized officials?	
	e. Whether change management procedure is being followed and documented?	
	f. Whether requirements are analyzed for feasibility and necessity?	
	g. Whether proper approval is being taken before making changes?	
	h. Whether changes are tested for correctness before implementing in production environment?	
3	Whether parameters of Operating System/RDBMS and Application Software are being changed/ updated as per the prescribed procedures and register to this effect is being maintained? (Not applicable in CBS branches)	

4	Whether all the transactions, except system generated, are authorized by an independent official?	
5	Whether database is physically secured? (Not applicable in CBS Branches)	
6	Whether the access to the application is restricted to the authorized officials only? (Not applicable in CBS branches)	
7	Whether the data is verified periodically in terms of storage space, performance tuning and back up. Give the following details:	
	i)Date of earliest data available	
	Ii)Total capacity of hard disk	
	iii)Free hard disk space	
8	In this context, review the response time of the system for different transactions.	
9	If the branch was migrated from one package to another after the date of last system audit, was the data integrity ensured.	
10	Whether adequate separation of duties is ensured for make checker concept?	
11	Whether Incumbent In charge periodically certifies/confirms that the financial powers of the various authorizing officials/end users are defined correctly in the system.	

12	Whether the guidelines with regard to checksum are being followed. What action the branch has taken in the event of difference in checksum. (Not applicable in CBS branches)	
13	Whether error messages, if any, in the screen are properly recorded in a Register and appropriate action taken?	
14	Review the adequacy of the procedures followed for implementing software patches/ periodical upgrades/ new version for application package as well as operating system.	
	Maintenance & Business Continuity Controls:	
1	Whether all the hardware items are covered under Warranty/Annual Maintenance Contract? Whether preventive maintenance schedule is being adhered to?	
2	Whether a Copy of AMC/Service Level Agreement is held in the Office?	
3	Whether the users are aware of the terms of AMC and the names and contact numbers of AMC Vendor?	
4	Whether the Software are being supported by the supplier vendor/In-house Development Team? Whether the contact numbers of the persons to be contacted in case of problem/break down is known to the users.	
5	In case any hardware item is taken out by the vendor for repair/ servicing, whether user ensures that the equipment does not contain sensitive data?	
6	Whether the users are familiar with the fall back procedures to be adopted in the event of power failure or fault in PC, Printer or any other peripheral?	
7	Whether users are aware of the procedures for restarting the work in the event of service interruption for various application packages running in the branch?	

8	Whether users are aware of the Security Policy guidelines of the Bank to the extent relevant to them.	
9	Whether Anti Virus Software is loaded in the systems? Whether data definitions and virus signatures are updated regularly? Give date of last such updation along with the source of updation (by vendor or through internet) and periodicity i.e. daily/weekly/monthly etc.	
10	Is the Anti Virus Software configured to check viruses from floppy/CD ROM/e-mail automatically?	
11	Check and report if any extraneous software is being used. Give details of such software (s) along with the PCs on which the same is loaded.	
12	Whether the users have been provided training in the area of their work?	
13	Whether license is held in respect of software being used by the Office/Branch.	
14	Whether the original Operating System, RDBMS & other Software packages are kept in a fireproof cabinet?	
15	Whether complete backup of Operating System/RDBMS and other application packages with current settings is held/maintained?	
16	Whether offsite backup is kept regularly on weekly basis? Give date of last such backup. (Not applicable in CBS branches)	
17	Whether all the columns of backup register are filled in properly. (Not applicable in CBS branches)	
18	Whether backup media is labeled and recorded? (Not applicable in CBS branches)	

19	Whether integrity/ readability of the backup is tested periodically? Comment on the method adopted for the same. Give date of last such testing. (Not applicable in CBS branches)	
20	Whether branch-wise inventory of Hardware/Software is being maintained and updated at Zonal Office Level?	
	Networking controls: **(Not applicable in stand alone environment)**	
1	Are there documented procedures for using the network?	
2	Has the responsibility and liability of network vendors been defined in the AMC Agreement, whether a copy of such AMC contract is held?	
3	Whether the inventory of network equipments e.g. hub, switch, router etc. is being maintained and updated regularly.	
4	Whether a network diagram illustrating the physical connections between the network equipments and computers had been prepared and approved by the Incumbent?	
5	Whether the networking equipments have been labeled to facilitate cross-reference to inventory register?	
6	If routers are installed, review the access controls to the routers.	
7	Whether the remote log-on through services such as FTP, TELNET etc. is disabled?	
8	Whether dial up access to RAS is logically controlled?	

9	Whether CBS node provided in the Office, if any, is physically separated and logically controlled? CBS node should not be used in any other network, report deviation if any. (Applicable only in CBS branches)	
10	Whether guidelines for e-mail usage are being complied with?	
11	Whether guidelines for internet usage are being complied with? Comment on the network downtime.	
12	Whether internet access is given to PC/System being utilized for some bank application having critical data? If so, what precautions are taken to protect against internet hazards?	
	<u>Operational Controls:</u>	
1	Whether the following reports are taken and scrutinized by the appropriate officials?	
	i) Exceptional Transactions Report.	
	ii)Rejected Transactions Report.	
	iii)Access Log	
	iv)Audit Trail, if any (non-financial transactions).	
	v)GL affected balances	
	vi)Active Users	

2	Whether the interest charged in the accounts is being checked/verified by the authorized official?	
3	Whether the interest rate revision is timely incorporated and authorized in the system. In case of delay, whether the differential interest for the intervening period is being appropriated.	
4	Whether morning checking is being done as per the Bank's guidelines.	
5	Whether the non-financial transactions e.g. limit enhancement, limit reduction, DP maintenance etc. are properly incorporated and authorized by the authorized officials of the Bank.	
6	Review the controls over the procedures adopted for data upload through external media e.g. salary credit through floppy etc. Whether such floppies are checked for viruses before using for processing? What are the controls for checking that the data is not entered more than once? Are compensatory controls in place in the form of checking of transaction by authorized officials?	
7	Whether the branch is maintaining any upload account in which some balance is still outstanding? Give details and explain the reasons for keeping such accounts. (Applicable only in CBS branches)	
8	Whether the transactions lying in the Proxy Account are reversed within 3 days? Review the outstanding transactions in Proxy Account for overdue entries. (Applicable only in CBS branches)	
9	Comment on the number of inter-sol transactions and the charges levied. Whether limited user IDs are permitted to pass such transactions? (Applicable only in CBS branches)	
10	Whether the signatures are being captured regularly and authorized in the system? Level of pungency in this regard be commented upon.	

	Review physical, logical, system and operational controls in respect of the following services rendered by the Branch, if any:	
1	Remote Access	
2	Tele Banking	
3	EDI	
4	Government Business	
5	CMS	
6	Depository	
7	SWIFT	
8	Internet Banking	
9	SFMS	
10	Whether access to ATM room is restricted to the authorized persons only?	
11	Whether AC installed in ATM room is giving the desired temperature control?	

13	Whether ATM room is clean?	
14	Whether ATM power back up is supported by UPS.	
15	Whether ATM card issue register is maintained and updated regularly and tallies with physical cards received in the branch?	
16	Whether control of ATM cards and PIN mailers (in case returned due to wrong address) with two different officials and proper record of the same is maintained and tallies with physical cards?	
17	Whether proper record of retained cards and lost/hot cards is maintained and tallies with physical cards?	
18	Whether after each month end, ATM audit rolls are kept in sealed envelope in joint custody?	
19	Comment whether security in ATM Room is in place.	
	Register Maintenance:	
1	Whether the following registers are being maintained, updated and scrutinized/checked.	
	a)Software problem Register.	
	b)Machine breakdown Register, recording downtime.	
	c)Users maintenance Register	

	d)Back up Register	
	e) Media stock movement Register.	
	f) Hardware/Software inventory management Register showing the configuration details and availability of Warranty/AMC.	
	g) Parameter Updation registers.	
	h) Daily arrangement registers.	
	i) Checksum Register.	
	J) Error Rectification Register (recording operational transactions).	
	k) ATM Register.	
2	IS AUDITOR'S OBSERVATIONS	
3	IS Auditor to comment/review overall IT governance in the branch/Office? Lacuna or gap is informed/indicated along with steps to be taken to plug it.	
	Adequacy of Hardware, Network and its redundancy.	