

Information System Audit of Banks

Compiled by Spandane

Index -Information System Audit of Banks

Para	Topic
1.0	Hardware installed at Data Centre / Branch
2.0	Installation of Computers
3.0	Server Farm / Room
4.0	Scanner
5.0	Fire Extinguishers
6.0	Physical Security
7.0	Insurance:(Electronic Equipment Policy)
8.0	Hardware Maintenance
9.0	UPS
10.0	Anti-Virus
11.0	Software
12.0	Software Maintenance
13.0	Back up
14.0	Data Purging
15.0	LAN Security
15.1	Login Controls
15.2	Password Controls
15.3	Data Access Controls
15.4	Terminal Controls
15.5	Temporal Controls
15.6	Dial up Controls
15.7	Back up Controls
15.8	Firewalls
16.0	Data Security
17.0	Registers
18.0	Print outs
19.0	Scanning
20.0	Miscellaneous

Para	Topic
21.1	Review of ATM Operations
21.2	ATM Cost Sheet
21.3	ATM Registers
22.0	Disaster Management
23.0	Rating
24.0	Major Irregularities requiring urgent attention

Definition of Information system Audit

	Information systems Auditing is a systematic process of collecting and evaluating evidence / information to access whether the information security systems
i	Safeguards assets effectively
ii	Maintain data integrity
iii	Achieve goals of the organization effectively,
iv	Result in efficient use of available information system resources.

Computer Process under CBS

Sr. No.	To confirm----
1	Whether day-begin has already been done by Data Centre?
2	Re-check on network to be done before service hours.
3	New user application forwarded by branch manager (also transfers, retirements, resignations)
4	End of Day hand over by branch
5	Exception and other reports

Scope of Information system Audit of Banks

Sr. No.		Branch	Data Centre	D. R. Centre
1	Hardwate Control			
2	Environmental Control			
3	Access Control			
4	Data Protection Control			
5	Data Access Control			
6	Network Control			
7	CommunicationControl			
8	Personnel Control			
9	Service Control			
10	Back up Control			

I S Audit of Branches

Sr. No.	Scope
1	Security - Hardware and Software
2	Hardware register, user register
3	Back up and Disaster recovery practices
4	Report circulation and authentication
5	AMC facilities & its monitoring
6	Voucher marking - transaction number
7	a) Revenue Test Check
	b) Availability of IS Policy, Disaster Management Policy
	c) Number of users attached to the branch vs. physically present and its reconciliation.

From:	Report	
	Bank	
	Location	Branch / Data Centre / D. R. Centre
	Subject	Information System Audit of Banks
	Date of Review	

Sr. No.	Particulars	Observations	
		Qty.	Average age
1.0	Hardware installed at Data Centre / Branch:		
	Item		
1.1	Computer System with Hard Disk		
1.2	Computer System without Hard disk		
1.3	Servers		
1.4	Thin-client		
1.5	Router		
1.6	Switches		
1.7	Hubs		
1.8	Modems		
1.9	Scanners		
1.10	Printer (Dot Matrix)		
1.11	Printers (Inkjet/Laserjet)		
1.12	Passbook Printers		
1.13	UPS		
1.14	Others		
1.15	Lease Line		
1.16	Dial up net work		
1.17	ISDN Lines		
1.18	Wire less Network		
1.19	LAN Cabling		
1.20			
1.21			
1.22			

2.0	Installation of Computers:	
➤	Refer Annexure-1/Computer Do's & Don'ts.	
2.1	Whether computers are maintained in dust free environment?	
2.2	Whether computers were kept clean?	
2.3	Whether separate electrical supply line has been provided for computer equipment with necessary circuit breakers?	
2.4	Whether computers have been housed in separate cabins or on kept at the counter with facility of locking?	
2.5	Whether earthing for electrical line is checked at periodic intervals? (Reading on the voltage meter on neutral points should show between 0-5 ampere)	
2.6	Whether Earthing of the building is checked at periodic intervals?	
2.7	Whether detailed map of the cable lay out including the hubs is available with the branch? (It will facilitate fast repairs to LAN cable faults)	
2.8	Whether HUBS have been installed in a secured place? (To avoid possible physical tampering)	
2.9	Whether LAN cables have been allowed to trail on the floor?	
2.10	Whether any heavy article is kept on the cables? (To avoid possible data loss)	
2.11	Whether EDP department monitors Volume / Space information periodically?	
2.12	Whether LAN Network diagram is available? (Branch/DC/DR)	

3.0	Server Farm/ Room:	
3.1	Whether server room is away from the main door, windows, passage and customer area?	
3.2	Whether server room is located not endangered by rain, wind, dust etc. which will reduce the life of the server?	
3.3	Whether AC provides adequate cooling and humidity for the server farm / room?	
3.4	Whether additional ACs has been installed to work in rotation with a Timer?	
3.5	Whether temperature measuring instrument and smoke & fire detectors has been installed in server room?	
➤	Ambient temperature normally recommended is 18° C.	
3.6	Whether server room is locked?	
3.7	Whether entry to server room is restricted?	
3.8	Whether the new user entry policy has been set, documented and evaluated regularly?	
3.9	Whether entry of outsiders to server room is approved by competent official?	
3.10	Whether record of visitors & reason for allowing access to server room has been maintained?	
3.11	Whether access is controlled through biometric or smart cards in order to prevent authorized access?	
3.12	Whether controlling devices are in working condition?	
3.13	Whether AMC has been given for maintenance of controlling devices?	
3.14	Whether audit trails of key card access systems	

	is checked daily?	
3.15	Whether failed logs are investigated?	
3.16	Whether Monitoring or Surveillance system (CCTV) has been installed in Data Centre?	
3.17	Whether numbers of cameras are adequate to cover the entire area?	
3.18	Whether recording is done simultaneously by all cameras?	
3.19	Whether control panel displays the images from all cameras in a single screen with a facility change over to the particular camera?	
3.20	Whether notice board namely 'Area is covered by CCTV' has been displayed in the data centre?	
3.21	How many days recording of CCTV are made available?	
3.22	Whether server has been installed in a room with atleast one wall of glass panel permitting the view from outside?	
3.23	Whether Data centre follows the Password Policy at all times?	
3.24	Whether is it supervised?	
➤	Refer Sr. No.15.2/ Password	
3.25	Whether System Administrator access is under the two factor access?	
3.26	Group Ids should not be made but only individual to pin responsibility. Whether complied?	
3.27	Whether server is password protected?	
3.28	Whether server room is maintained clean and not used for storage of any record?	
3.29	Whether printer has been kept in server room?	

3.30	Whether record of failure of lease line /dial up net work has been maintained and analyzed?		
4.0	Scanner:		
4.1	Whether scanner has been kept under lock, when not in use?		
4.2	If scanner is attached to a particular terminal, whether the said terminal is password protected?		
5.0	Fire Extinguishers:		
5.1	Fire extinguishers of CO2 inert gas type can only be used on computer equipment (in the event of fire breaking out)	Type to be stated.	
5.2	Whether fire extinguishers have been installed?	Yes	No.
5.3	If yes, whether in up to date condition?		
5.4	Next service due on		
5.5	Whether staff members have been given adequate training to use fire extinguishers in case of need?		
6.0	Physical Security:		
6.1	Whether computer items are properly numbered and entered in the dead stock register?		
6.2	Whether machines under warranty period are marked separately with date of purchase?		
6.3	Whether physical verification of computers etc. is done periodically?		
6.4	If yes, date of last such verification & by whom?		
6.5	Whether any discrepancy was noticed?		

6.6	Whether any items have been sent for servicing / repairs?		
6.7	Whether any item is in irreparable condition?		
6.8	Whether any surplus hardware is lying with the branch? With whom?		
7.0	Insurance:(Electronic Equipment Policy)		
7.1	Whether insurance policy has been taken?		
i	Insurance Company		
ii	Policy Number		
iii	Sum insured	Rs.	
iv	Valid up to		
v	Risk covered		
vi	Premium	Rs.	
7.2	Whether movement of hardware from one office to another office is informed to Insurance company?		
7.3	Details of pending claims:		
i	Date of incident / loss etc.		
ii	Loss estimated	Rs.	
iii	Survey carried on		
iv	Existing status		
8.0	Hardware Maintenance:		
8.1	Whether service contract (AMC) has been given for following items?	Yes / No	Period
i	Computer System with Hard Disk		
ii	Computer System without Hard disk		
iii	Servers		
iv	Thin-client		

v	Router		
vi	Switches		
vii	Hubs		
viii	Modems		
ix	Scanners		
x	Printer (Dot Matrix)		
xi	Printers (Inkjet/Laserjet)		
xii	Passbook Printers		
xiii	UPS		
xiv	Others		
xv	Lease Line		
xvi	Dial up net work		
xvii	ISDN Lines		
xviii	Wire less Network		
xix	LAN Cabling		
8.2	Whether preventive maintenance is done?		
8.3	If yes, what is the frequency?		
8.4	Date of last such maintenance		
8.5	Comments on quality of service ---- Preventive		
	Comments on quality of service ---- Breakdown		
8.6	Whether a log-sheet of hardware (Computers, UPS & Printers) problems is maintained?		
8.7	If yes, whether updated regularly?		
8.8	Whether visit report of service personnel are		

	reviewed by Branch official, EDP department?	
8.9	Whether name, address, telephone numbers, Name of the concerned engineer etc. is noted in the said register?	
8.10	Who is the system administrator of the Branch / Data Centre / D. R. Centre?	
9.0	UPS:	
9.1	Whether power supply has been provided to computers through UPS?	
9.2	Whether UPS room is locked?	
9.3	Whether entry to UPS room is restricted?	
9.4	Whether UPS system is free of load from electrical equipments such as fan, AC, tube lights etc.?	
9.5	Whether batteries are kept for charging after office hours?	
9.6	Whether periodic checking of UPS & batteries is done?	
9.7	Whether record to that effect has been kept?	
9.8	What is the duration for which computer system can function on UPS?	
9.9	When UPS was put to use last?	
9.10	What was the approx. duration?	
9.11	Whether register has been maintained to record power failure?	
9.12	Whether loss of data is confirmed after every power failure?	

10.0	Anti-Virus:	
10.1	Whether Anti-virus software is used?	
10.2	Details.	
10.3	Whether this is the licensed copy of software?	
10.4	Whether the said version is latest?	
10.5	Date of last updating.	
10.6	Whether the anti-virus program is activated at fixed time?	
10.7	Whether Anti-virus software has been loaded even on PCs with hard disk?	
11.0	Software:	
11.1	Which software does the branch use?	
11.2	Whether it is latest?	
11.3	Whether it is authorized copy?	
11.4	Whether MS-Office installed at the branch is an authorized copy of software?	
11.5	Whether any unauthorized software is installed at the branch? To Specify.	
11.6	Whether any games have been installed in server / hard disk?	
11.7	Whether any Authorized Freewares is installed?	
11.8	Whether any unauthorized Freewares have been installed?	
11.9	Whether latest service pack for operating system software (OS) has been installed?	

12.0	Software Maintenance:	
12.1	Who is responsible for software maintenance?	
13.0	Back up:	
13.1	Whether back up is taken of data, index & program?	
13.2	If yes, when?	
13.3	Whether back up register is kept?	
13.4	Whether signed by concerned officer and time is recorded?	
13.5	Whether Hard_disk-to-Hard_disk back up is taken?	
	If yes, when?	
13.6	Where back up cartridges are stored in fireproof cabinet?	
13.7	Whether back up is sent to HO, locker, nearby branch etc.?	
13.8	If yes, whether record is kept?	
13.9	Whether back up is taken home by Manager?	
13.10	If back up is taken on floppies, whether floppies are formatted periodically and replaced at regular intervals?	
13.11	Whether back up has been taken in latest device?	
13.12	Whether back up was tested for restoration?	
13.13	Whether monthly back up is taken?	
13.14	Whether yearly back up is taken?	
13.15	Whether Disaster Recovery and Business Continuity Plan has been documented and	Refer Para 22

	tested periodically?	
14.0	Data Purging:	
14.1	Whether top management authorizes data purging?	
14.2	Whether back up before and after purging has been taken?	
14.3	If yes, whether tapes have been properly labeled indicating the date, period & other details?	
14.4	Where purged data has been stored? (On the server in another volume or on the node with hard disk or on a standalone PC)	
14.5	Whether access to the purged data has been restricted?	
14.6	Whether all the required reports before purging are printed and filed?	
14.7	Whether manual record of the purging has been kept?	
14.8	When purging was done last?	
15.0	LAN Security:	
	Whether following controls are observed?	
15.1	Login Controls:	
i	Whether User Management norms have been defined and documented?	
ii	Whether users are approved by HO?	
➤	Names of all staff members should be incorporated in User Master.	
➤	Login should be done by employee code. It is suggested to have uniformity by inserting short name as initials. e.g. DVP (First name, father's/husband's name and surname)	

➤	Auto Log off should be activated in case Login is not done for 2 days. Activation rights should be with HO EDP only.	
iii	Whether User Approval application is maintained?	
iv	Whether users are created by HO EDP?	
v	Whether all users are uniquely identified?	
vi	Whether unlocking of accounts of users whose accounts are locked is carried out after obtaining unlocking requests & duly approved by competent authorities?	
vii	After how many unsuccessful attempts at login, a user is locked out?	
viii	Any restriction on number of logins in a day?	
ix	Whether the duration of inactivity before screen gets locked has been stipulated?	
x	Whether any staff member possesses multiple levels or more than one user-id in the system?	
xi	Whether any dummy user-id has been created in the system?	
xii	Whether branch has suspended user-ids of staff on long leave, transferred, deputed for training etc?	
xiii	Whether branch obtains acknowledgement from every user at the time of creation / allotment of user-ids?	
15.2	Password Controls:	
i	Whether Password is masked at the time of entry?	
ii	Whether system compels the user to change the Password when he logs in for the first time?	

iii	Whether user is disabled on entering erroneous password on three consecutive occasions.	
iv	What is the frequency stipulated for change of password?	
v	Whether Password expires automatically after stipulated number of days?	
vi	Whether system ensures that Password is alphanumeric? (Preferably)	
vii	Whether system ensures that Password is alphanumeric & one special character? (Preferably)	
viii	Whether system ensures that login id and Password is not he same?	
ix	Whether system ensures that changed Password is not the same as last 12-15 Passwords?	
x	Whether system ensures that the Password should of minimum 8 characters and maximum 12 characters?	
xi	Whether Password policy has been documented?	
xii	Whether branch has maintained Password Issue and Password Changes Registers.	
xiii	Whether branch official reviews the user login status report and record his remark in that regard in Password Issue register?	
xiv	Whether undertaking is obtained from the staff for maintaining secrecy and confidentiality of the password?	
xv	Whether guessable passwords have been listed to debar its use?	
xvi	Whether user Id is case sensitive? (Preferably)	

xvii	Whether Password is case sensitive? (Preferably)	
xviii	Whether copy-paste of user id and password has been disabled? (Preferably to be done)	
15.3	Data Access Controls:	
i	Whether users are given only the rights that are essential for carrying out their duties?	
15.4	Terminal Controls:	
i	Whether computer system has been instructed to restrict particular user to particular terminals only?	
15.5	Temporal Controls:	
i	Whether the user and terminal is provided with computer facility only during specified times in a working day?	
15.6	Dial up Controls:	
i	Whether dial back provision is made in case outsider is allowed to access a computer through telephone connection?	
15.7	Back up Controls:	Refer Sr. No. 13
15.8	Firewalls:	
i	Whether comprehensive list of what should be allowed / disallowed through the Firewall has been compiled, approved and kept up to date?	
ii	Where do you place firewalls?	

➤	The placement is situation specific and the auditor needs to be convinced about the logic of the decision.	
iii	How do you secure them against unauthorized access from internet, extranet and intranet users? e.g. Are inner firewalls placed around all critical, financial and transactional systems?	
➤	The placement is situation specific and the auditor needs to be convinced about the logic of the decision.	
iv	Is the firewall placed in between the network router and network or given application?	
➤	This is the minimum security level to be achieved by such a location in addition to its proper configuration.	
v	Whether entry and exit through any network port not required by the organization has been prevented?	
➤	Permitting entry through not required ports is leaving the back door open.	
vi	Whether firewalls are updated at regular intervals?	
vii	If yes, How often?	
viii	Is it updated when a patch is available?	
ix	What initiates a review?	
➤	Firewalls too need regular updation like the anti virus files which have to be updated for the new signature list for the software to use.	
x	Whether ingress and egress filtering is used?	
xi	Whether you follow the filtering rules?	
	If yes, Produce the list.	
xii	If users are allowed to connect from the internet to the internal network, whether access is restricted to either a virtual private network (VPN) or an encrypted software session? How is it restricted?	

➤	The Auditor should be convinced by the information systems engineer about the security assurance in such a situation.	
xiii	Whether access to the management interfaces of routers, firewalls and other network appliances has been adequately secured? e.g. Are these devices are also subject to appropriate passwords policy enforcement or whether two factor authentication has been employed?	
➤	All security measures would be defeated if the set up of the firewall itself was not under a secure procedure.	
16.0	Data Security:	
16.1	Whether branch parameters, subsystem codes, standing instructions and holiday file have been properly created / updated by EDP/Data Centre?	
16.2	Whether interest tables have been updated?	
16.3	Whether slab rates have been up dated?	
16.4	If yes, whether checked by officer & record to that effect has been kept?	
16.5	Whether any changes in the data such as DP, special instruction etc. are authenticated by branch officials and record to that effect is kept?	
16.6	Whether copies of HO Circular for change in interest rates, service charges etc. are readily available?	

17.0	Registers:				
17.1	Whether following registers are maintained & if yes, whether up to date?	Whether maintained?	Whether up to date?		
i	Dead stock register for computers				
ii	Back up register				
iii	Back up movement register				
iv	Hardware problems register				
v	Software problems register				
vi	Due date diary for AMC				
vii	Software release updating register				
viii	Visit register for AMC personnel				
ix	Power failure register				
x	User register				
xi	Computer data change register				
xii	Register of computer consumables such as floppies, cartridges, tapes, ribbons, printed stationery etc.				
xiii	Register of destroyed floppies				
xiv	Password Issue				
xv	Password Changes				
xvi					
xvii					
18.0	Print outs:				
18.1	Whether following print outs are taken, checked, signed and filed properly?	Print outs	Check ing	Signi ng	Filing
i	Day book				
ii	Scroll				
iii	Supplementary -Cash				
iv	Supplementary - Clearing				
v	Supplementary - Transfer				

vi	Trial balance				
vii	Balancing statements				
viii	Debit balance report				
ix	Exception transaction report				
x	All O. K. Statement				
xi	General ledger				
xii	Loan ledger				
xiii	Deposit ledger				
xiv	Parameter file print out				
xv	Master file print out				
xvi	Account opening. Closing, modification (relevant master)				
xvii	Audit trail print out				
18.2	Whether prescribed reports are printed regularly?				
19.0	Scanning:				
19.1	Whether signature are scanned & authorized regularly?				
		SB	CD	CC/ OD	TDR
	Running account number				
	Signature scanned up to				
	Confirmed up to				
19.2	Whether scanned signatures of dormant account are deleted?				

20.0	Miscellaneous:	
20.1	Whether staff is rotated on regular basis?	
20.2	Whether stamp is affixed on cheques, credit slips, withdrawal slips, vouchers etc. indicating transaction number, scroll number and initials of operating staff?	
20.3	Whether consumables are kept under lock & key?	
20.4	Whether consumables are inspected periodically?	
20.5	If yes, date of last inspection	
20.6	Whether internet connection has been provided?	
20.7	If yes, how control is exercised on its usage?	
20.8	Details of time utilized since April	
20.9	Whether all users' manuals have been numbered & entered in Register to monitor the movement?	
21.0	ATM:	
21.1	Review of ATM Operations	Refer Annexure - 2
21.2	ATM Cost Sheet	Refer Annexure - 3
21.3	ATM Registers	Refer Annexure - 4
22.0	Disaster Management:	
22.1	Whether Bank has a Disaster Management Policy?	
22.2	Whether Disaster has been defined?	
22.3	Where Disaster site has been located?	
22.4	Whether Disaster site complies the following:	
i	Whether located in different seismic zone? (i.e. different earthquake zone)	

Annexure-1 forming part of IS Audit of Banks. (Sr. No. 2)

From:	Report	
	Bank	
	Branch	
	Subject	Computer Do's & Don'ts
	Date	

Sr. No.	Observations	Reply
A	On computer System	
	Whether you-----	
1	Keep your computer system in a cool, dry and dust-free environment?	
2	Ensure that the power switches in a system unit, monitor and printer are in the OFF position before switching on the mains?	
3	Switch off the monitor, system unit and the printer, before switching off the mains?	
4	Clean the computer work area everyday; cover your system at the end of the day.	
5	Keep your system away from room walls to ensure proper airflow around the computer?	
6	Park the hard disk and then shift it, when the unit needs to be transferred from one side to another?	
7	Handle the floppy drive lever gently?	
8	Ensure that there is no diskette in the floppy drive before switching off the system unit?	
9	Clean the keyboard regularly?	
10	You use vacuum cleaner to clean keyboards to extract the dust collected in between the keys?	
11	Use mouse pad?	

12	You make sure to place the mouse on a clean surface in case you do not have mouse pad?	
B	Printer	
	Whether you----	
1	Choose a flat, sturdy surface with enough room for the paper to flow freely in and out of the printer? (If you use continuous fan-fold paper, you will need space behind the printer (or underneath with its bottom-feeding) for a stack of paper)	
2	Position the printer so that its connections namely, power cord and computer cable will not interfere with the paper flow?	
3	Position the feed paper stack and the printed output such that one does not interfere with the flow of the other?	
4	Position the feed paper stack such that the paper advances straight up? (If the stack is slightly away or off-centre, it causes the paper to mis-feed)	
5	Use the paper thickness lever (if your printer has one) appropriately?	
6	Use the paper thickness recommended in the printer manual?	
7	Turn the power off, unplug the power cord and disconnect the printer cable when performing any kind of cleaning operation?	
8	Clean the insides of the printer? (To clean the printer, remove the printer cover and the ribbon cartridge. To clean the inside of the printer, use a soft brush to whisk lint and dust away from the print head area. The outside of the printer case can be cleaned when needed with a damp rag and alcohol. A vacuum cleaner is very useful for sucking out the paper particles from the inside of the printer.	
9	Use the printer cover? (It is a dust protection cover, noise buffer and paper cutter, all in one)	

10	Turn off the power and slide the print head to the left edge before removing the old cartridge> (This will prevent the printer head cable from getting damaged)	
C	Whether you---	
1	Eat or drink near the computer?	
2	Smoke inside the computer room? (Smoke is injurious to computer health also)	
3	Allow direct sunlight to fall on your computer? (It is necessary to avoid warping of magnetic media)	
4	Run any electric equipment like a vacuum cleaner in the vicinity of the computer when it is on?	
5	Switch on the system with a data floppy in the drive?	
6	Insert or remove the diskette when the drive select indicator is glowing?	
7	Switch off the system when the hard disks drive, i.e. when the indicator is glowing?	
8	Strike the keys as hard as those of a manual typewriter? (Keyboard keys soft touch)	
9	Rest your hands on the keyboard?	
10	Keep anything on the keyboard?	
11	Use the keys after switching off the system?	
12	Stretch the cable at the keyboard end? (This may lead to snapping of the wires inside the cable)	
13	Turn the paper feed knob when the printer is printing.	
14	Turn the platen knob in the reverse direction?	
15	Move the print head manually when the printer is on?	
16	Pull the mouse cable?	
17	Expose the mouse to excessive moisture?	
18	Subject the mouse to impact? (Do not let it fall and do not place the keyboard on it.)	

Annexture-2/ Review of ATM Operations (Sr. No. 21)

From:	Report	
	Bank	
	Branch	
	Subject	Review of ATM Operations
	Date of Review	

**1 Whether following ATM Registers are maintained & if yes, whether updated?
Refer Annexture-4 for Formats of ATM Registers)**

Sr. No.	Name	Whether maintained?	Whether updated?
1.1	ATM Card Applications Issued		
1.2	ATM Card Applications received		
1.3	ATM Cards received from HO		
1.4	ATM Cards Issued		
1.5	ATM Complaints Register		
1.6	ATM Cards stolen, lost, damaged		
1.7	ATM Hot Card register		
1.8	ATM Cash balance register		
1.9	ATM Daily Transaction Register		
1.10	ATM Deposit Register		
1.11	ATM Suggestion register		
1.12	ATM Breakdown register		
1.13	ATM Cost Sheet (Refer Annexture-3)		

2.0	Reconciliation of ATM Cards etc.	
2.1	ATM applications issued.	
2.2	ATM applications received. (2.3+2.4)	
2.3	ATM applications not forwarded to HO.	
2.4	ATM applications forwarded to HO. (2.5+2.6)	

2.5	ATM Cards received from HO. (2.8+2.9)		
2.6	ATM applications pending at HO.		
2.7	Whether confirmation obtained of Sr.no.2.6		
2.8	ATM Cards issued to customers.		
2.9	ATM Cards not issued to customers.		
3.0	ATM Dept. Administration at branch:		
3.1	Whether officer has been designated to look after ATM operations?		
3.2	Whether ATM card & PIN is forwarded to branch?		
3.3	Whether PIN is forwarded to customer directly?		
4.0	Safe Custody of ATM cards:		
4.1	Where ATM Cards are kept over night?		
4.2	Whether ATM cards are kept under lock & key during the day?		
4.3	Whether specimen signature is verified while issuing ATM Card?		
5.0	Cash Balance Reconciliation:		
5.1	What time ATM reports are printed and cash is verified?		
5.2	ATM cash balance as per GL dated		Rs.
5.3	ATM cash balance as per Register.		Rs.
5.4	Difference if any		Rs.
5.5	Reasons / Action:		
6.0	ATM Cards usage Statistics:	ATM is in use from	
6.1	ATM withdrawals till end of last month: Nos.		Average:
6.2	ATM Withdrawals in last one month		Nos.
6.3	Number of days ATM was not operative?		Days
6.4	Max. ATM Cash withdrawal in a day?		Rs.
6.5	Number of Saving Bank operative accounts?		

6.6	Number of ATM Cards issued & % to 6.5	
-----	---------------------------------------	--

7.0	Other Important Issues:	
7.1	Whether ATM is covered under AMC?	
7.2	If yes, AMC valid up to	
7.3	Whether Branch officials have the contact numbers of service providers readily available?	
7.4	Whether ACs installed in ATM Cabin is covered under AMC?	
7.5	If yes, AMC valid up to	
7.6	How many ACs have been installed in ATM Cabin?	
7.7	Whether Timer has been installed?	
7.8	If yes, whether Timer is in working condition?	
7.9	Whether Counter has been provided in ATM Cabin?	
7.10	Whether Privacy has been ensured for ATM Cabin?	
7.11	Whether separate security guard has been deputed for ATM?	
7.12	Whether ATM cabin is kept clean?	
7.13	Whether Bank's Deposit/Loans schemes are displayed on ATM wallpaper / in ATM Cabin?	
7.14	Whether ATM banner has been displayed at the branch?	
7.15	Whether HO has given ATM Card Issue Target?	
7.16	If yes, No. of ATM cards to be issued during the year.	
7.17	If No, whether Branch has fixed the Target internally?	
7.18	If yes, No. of ATM cards to be issued during the year.	
7.19	Whether Insurance Policy has been taken in respect of ATM?	
7.20	If yes, Sum insured & Insurance Policy valid up to	
7.21	Whether HO has fixed ATM Cash Retention limit?	

7.22	If yes, whether letter to that effect is on record?	
7.23	If no, How much maximum cash balance is kept in ATM?	
7.24	Whether cash bundles have been stored properly to facilitate cash verification?	
7.25	Whether the branch has kept sufficient ATM Rolls & other stationery?	
7.26	Who is aware of ATM Password?	
7.27	Whether Password has been given to two officials, broken in to 6 digits each?	
7.28	Whether ATM pamphlet is printed by branch?	
7.29	If yes, whether kept at counter for distribution to customers?	
7.30	Whether Staff is aware about ATM parameters such as maximum amount, no. of withdrawals per day, charges etc.	
7.31	Whether facility of 'Auto Credit 'is offered?	
➤	This facility should be discontinued to avoid fraud.	

Annexure-3 /ATM Cost Sheet (Refer Para 1.13) of Annexure 2 above.**ATM Cost Sheet for the period**

Sr. No.	1.0 Capital Investment	Avg. Life in years	Original cost Rs.	Depreciation % On SLM	Depreciation Rs.
1.1	ATM	3		33.33	
1.2	ATM software	3		33.33	
1.3	Air Conditioners	5		20.00	
1.4	Timer	3		33.33	
1.5	Civil work	5		20.00	
1.6	Glass door	5		20.00	
1.7	Shutter	5		20.00	
1.8	Premises	40		02.50	
1.0	Total				

2.0	Variable Expenses:				
2.1	ATM Cards				
2.2	Electricity:				
	➤ AC (48 units per day) @				
	➤ Tube light (1 unit per day)				
2.3	ATM Stationery				
2.4	Security guard charges				
2.5	Rent / Society charges				
2.6	Advertisement				
2.7	Prorata Staff Cost				
2.8	Insurance premium				
2.9	AMC-ATM				
2.10	AMC-Air conditioners				
2.11	Sweeper Charges				
2.12	Depreciation				

2.13	ATM charges paid to other banks.			
2.0	Total			

Annexture-4 / Formats of ATM Registers (Para 1 of Annexture-2 above)

01-ATM Card Applications Issued

Sr. No.	Date	Name	Address	A/C No.	Issued by	Received on	OFF Sign.	Remark

02-ATM Card Application Inward Register

Sr. No.	Inward No.	Date	A/C No.	Name	Address	Sent to HO on	OFF. Sign.	
							1	2

03-ATM Cards received from HO

Send to HO		Received from HO		Balance applications	Rejected	Pending
Date	No. of applications sent	Date	No. of cards received			

04-ATM Card Issued / Duplicate Card issued Register

Sr. No.	Issue date	ATM Card No.	A/C No.	Name	OFF Sign.		Customer Sign.	Inward No.
					1	2		

05-ATM Complaint Register

Date	ATM Card No.	A/C No.	Name	Nature of Complaint	Action taken	OFF Sign.	
						1	2

06-ATM Card Lost/ Stolen/ Pin Forgotten
--

Sr. No.	Date	ATM Card No.	A/C No.	Name	Reason	OFF Sign.		Action taken
						1	2	

07-ATM Hot Card Register

Date	ATM Card No.	A/C No.	Name	Reason	OFF Sign.		Action taken
					1	2	

08-ATM Cash Balance Register

Date	Cash: Retention Limit Rs.			OFF Sign.	
	Deposit	Payment	Closing Balance	1	2

09-ATM Daily Transactions Register

Date	On Line		OFF Line		Deposits by customers					
	A/C	Rs.	A/C	Rs.	Cash		Cheque		Total	
					A/C	Rs.	A/C	Rs.	A/C	Rs.

10-ATM Deposit Register

Sr. No.	Date	Time	ATM Packet No.	ATM Card No.	A/C No.	Name	Cash Rs.	Cheque Rs.	OFF Sign.	
									1	2

11-ATM Suggestions Register

Date	ATM Card No.	A/C No.	Name	Suggestion	Action	OFF Sign.	
						1	2

12-ATM Break down / Failure Register

Sr. No.	Date	Complaint No.	Complaint	Down From	Down To	Complaint given by	Solved on	OFF Sign.	
								1	2

RESERVE BANK OF INDIA

www.rbi.org.in

RBI/2009-10/83

UBD. CO.BPD.(PCB).MC.No. 9 /12.05.001/2009-2010 July 1, 2009

Chief Executive Officers of All Primary (Urban) Co-operative Banks

Dear Sir

**Master Circular
Inspection & Audit Systems in
Primary (Urban) Co-op. Banks**

Please refer to our Master Circular UBD.BPD.(PCB).MC.No.9 /12.05.001/2008-09 dated July 1, 2008 on the captioned subject (available at RBI website www.rbi.org.in).The enclosed Master Circular consolidates and updates all the instructions / guidelines on the subject up to June 30, 2009.

Yours faithfully**(A. K. Khound)****Chief General Manager**

Urban Banks Department, Central Office, 1 Floor, Garment House, Worli, Mumbai - 400 018

Phone: 022 - 2493 9930 - 49, Fax: 022 - 2497 4030 / 2492 0231, Email:

rbiubd@giasbmol.vsnl.net.in

Master Circular
on
Inspection & Audit Systems
in
Primary (Urban) Co-operative Banks
(Updated up to 30 June, 2009)
(The Master Circular is available at RBI website www.rbi.org.in
and may be down loaded from there)

RESERVE BANK OF INDIA

Urban Banks Department,

Central Office, Mumbai.

5 AUDIT FOR ELECTRONIC DATA PROCESSING SYSTEM:

5.1 Primary (urban) co-operative banks which have **partially / fully computerised their operations should introduce EDP audit system on perpetual basis**. In case such banks have an independent Inspection & Audit Department, an EDP audit cell should be constituted as part of their Inspection and Audit Department to carry out EDP audit in branches/offices having computerised operations. However, those primary (urban) co-operative banks, which do not have an independent Inspection & Audit Department, should create a **dedicated group of persons**, who, when required, can perform functions of an **EDP Auditor**. The overall control and supervision of these EDP Audit Cells should be vested in the Audit Committees. In this regard, all primary (urban) co-operative banks having fully/ partially computerised operations should ensure to comply with the norms stipulated in the succeeding paragraphs.

5.2 A team of competent and motivated EDP 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. EDP auditors' technical knowledge should be augmented on a continuing basis through deputation to seminars/conferences, supply of technical periodicals and books etc.

5.3 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.

5.4 Major factors which lead to security violations in computers include 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. These loopholes may be plugged by:

5.4.1 strengthening physical, logical and procedural access to system;

5.4.2 introducing standards for quality assurance and periodically testing and checking them;
and

5.4.3 screening employees prior to induction into EDP application areas and keeping a watch
on their behavioral pattern.

5.5 There is a need for formal declaration of system development methodology, programming and documentation standards to be followed by the bank, in the absence of which quality of system maintenance/improvement might suffer. EDP auditors should verify compliance in this regard.

5.6 Contingency plans/procedures in case of failure of system should be introduced/ tested at periodic intervals. EDP auditor should put such contingency plan under test during the audit for evaluating the effectiveness of such plans.

5.7 Every bank should have a manual of instructions for their inspectors/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.

5.8 An appropriate control measure should be devised and documented to protect the computer system from attacks of unscrupulous elements. Before introducing an EDP 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 EDP application.

5.9 In order to ensure that the EDP 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.

5.10 While engaging outside computer agencies, banks should 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/inputs given to such outside agencies.

5.11 Entire domain of EDP 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 EDP department should be reviewed by senior management at periodical intervals.

5.12 In order to bring about uniformity of software used by various branches/offices there should be a formal method of incorporating change in standard software and it should be approved by senior management. Inspection and Audit Department should verify such changes from the view-point of control and for its implementation in other branches in order to maintain uniformity.

Compiled by CA. Sudhir Vaidya \ Tuesday, June 22, 2010

